



Vulnerabilities in the Internet

Jaap Akkerhuis
jaap@sidn.nl



Disclaimer

- Simplistic generalizations
 - Not a network architecture course
 - Not a DNS course
- Touching only some points
 - Broad overview, not limited to 11th Sept events
- More analysis needed
 - Especially on details
- Terminology Internet related

Overview

- Two perceptions of the event
- Effects of the network damage
- ISP experiences
- TLD DNS vulnerabilities
- Closing remarks

Personal experience

- Sister in Manhattan (Houston)
- Was impossible to reach by phone
- E-mail took less than 7 minutes
 - 2 minutes to provider, 5 to my inbox
 - Clock skew?
 - *Everything is ok*
- Big failure: Phone system

Honeyman's Experience

- University of Michigan
 - Networking, cryptography, smart cards
- Got called
- No www.cnn.com or similar
- No Television, used Radio
- Big failure: Internet

What was going on?

- The network was out?
 - Cnn.com is an end point
 - Much more traffic then usual
 - http is transaction oriented
 - E-Mail is lightweight
 - Easy to route
- Phone was out?
 - Not really (8 hours)
- Perception

Measurements

- Matrix.net (MIDS) monitors continuously
 - Last 14 years
- View of the world from Austin Texas
 - 60,000 sites every 15 minutes
 - beacon list contains over 10,000 entries
 - ICMP ECHO (PING) and HTTP
 - probes from 100 points around the world
- Data supplied Peter Salus

Legenda

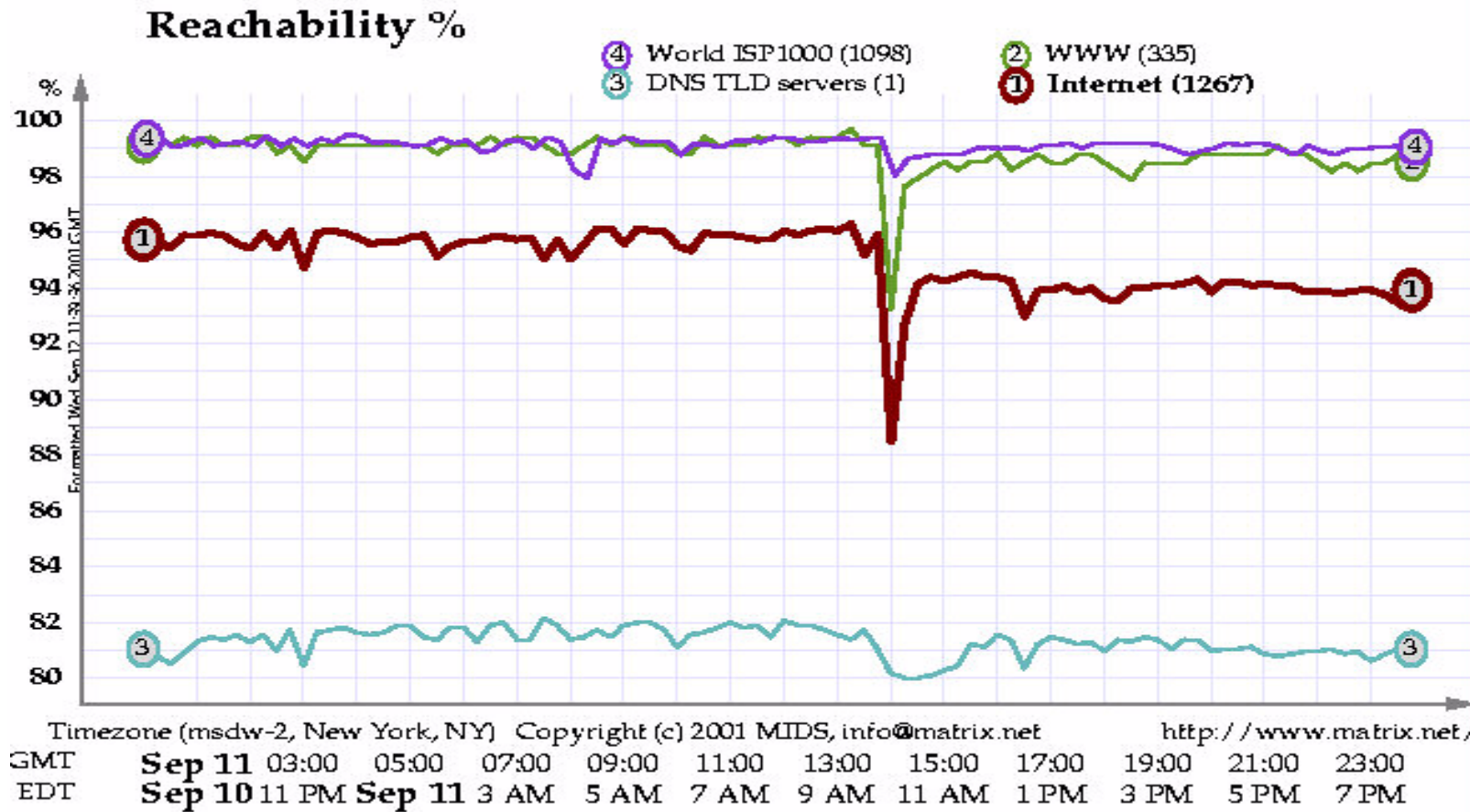
1: World ISP 1000

2: WEB

3: DNS TLD Servers

4: Internet

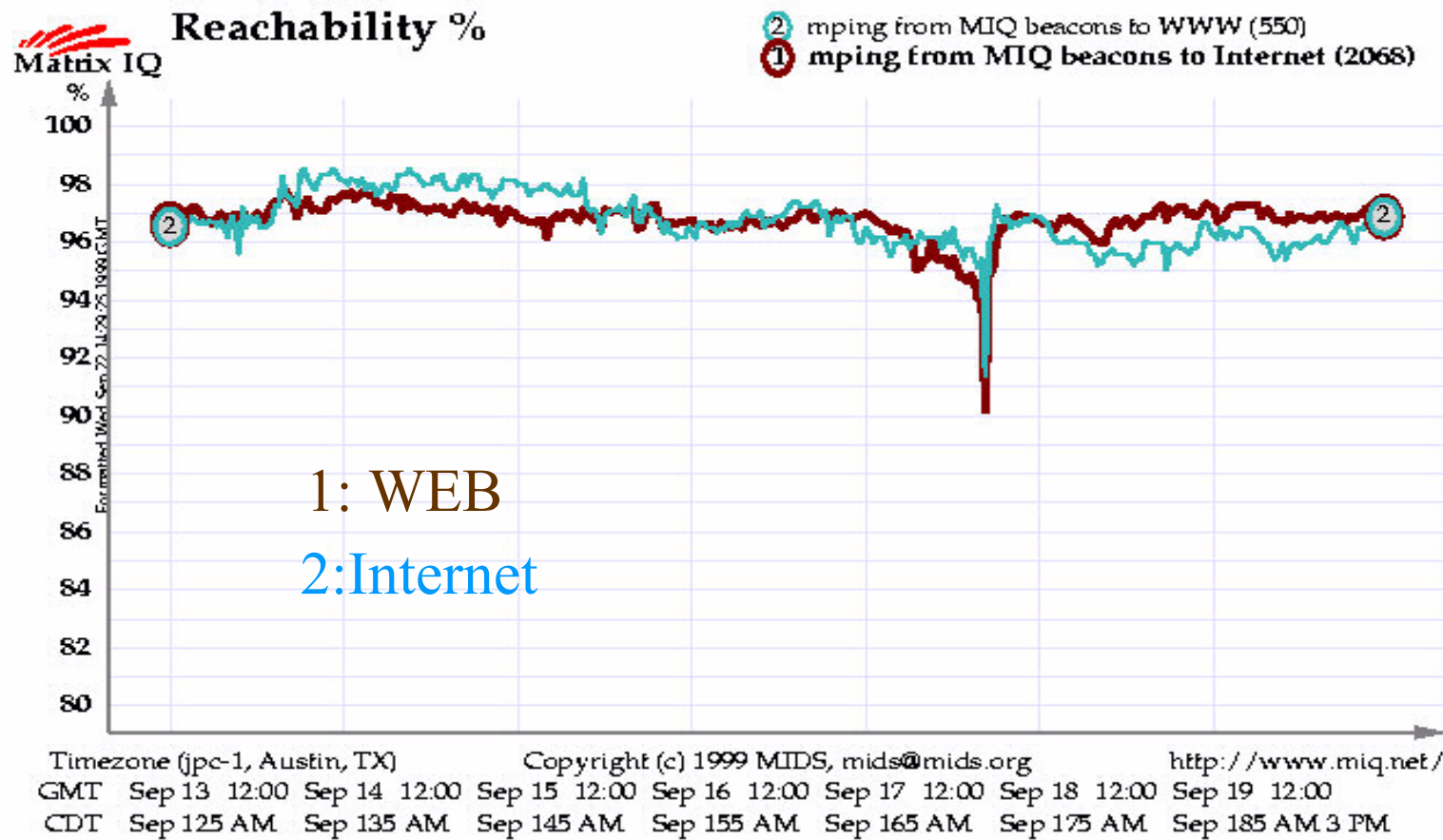
The Attack



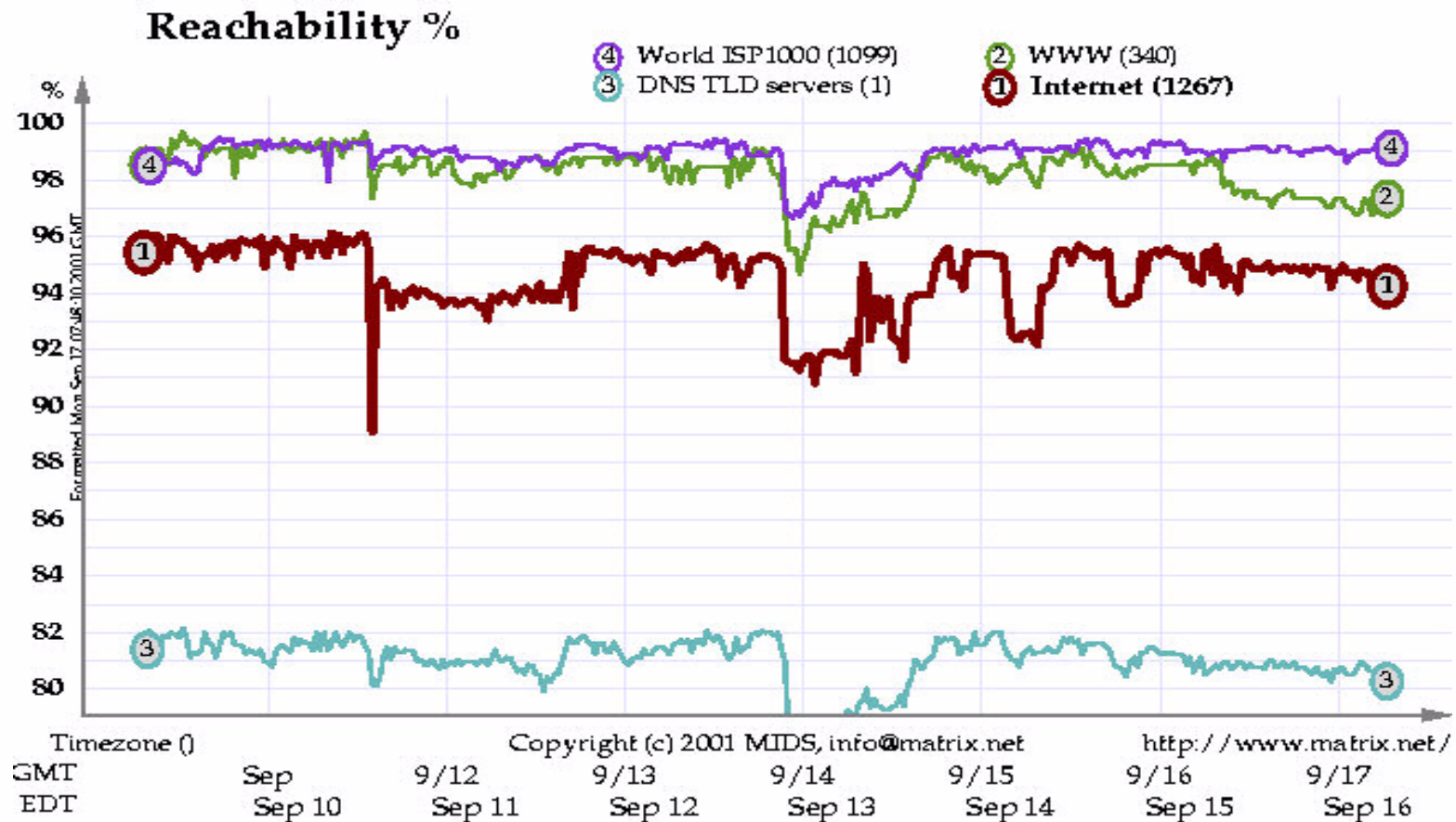
Effects

- WTC was major communication hub
- Telehouse (NY IX) close to WTC
- Lots of lines went out
- Rerouting takes some time

Hurricane Floyd



Events surrounding 11 Sept.



Events following 11th

- Anticipating power failure at Telehouse
 - ISPs set up extra peering at exchanges
 - Big operators helped out competitors
 - Extra multi homing by various ISPs

Comparable Outage: AMS-IX

- Amsterdam Internet Exchange (July 2001)
 - one of the major European IXs
- Problems
 - Two out of three locations broke down
- Hardware problems
 - Triggered by specific multi vendor combinations
- Took about a week to solve

Phenomena in Europe

- Medium sized Dutch ISP
- Big international ISP

Experiences ISP–W

- Description of operation
 - Medium sized Dutch ISP
 - 10 year in business
 - Transit with Telehouse (Broadway 25)
 - Major peering as well
 - Hosting farm at Telehouse
 - Minor peering at AMS-IX

Experiences ISP–W

- Extra measures
 - More peering & alternative transit
- Result
 - Transit OK
 - Hosting farm 1 week out

Experiences ISP–W

- Lessons learned
 - Network designed with redundancy
 - Need to think about more than the network security
- Transatlantic cable cut (3 weeks ago) was worse
 - 56 hours down

Reflections by *BIG* ISP on 11th

- Lots of extra transit
 - Need to be flexible
 - Strong arm the CFO
- Lots of multi homing set up
 - Grow of routing tables (20%)
- Not always effective
 - Routing policies of other ISPs
 - Router memory exhaustion

Reflections by *BIG* ISP

- Costs of redundancy policies
 - Threefold redundancy in transatlantic cables
 - *In the end, it's all economics*
- Transit at internet exchanges
 - Single point of failure
- Routing aggregations policies (Ripe NCC)
 - Trims size of routing tables
 - Uses more IP address space

TLD DNS Vulnerabilities

- DNS: Hierarchical distributed structure and name resolving
- Specific examples are neutral
 - using .nl, .de, .uk, .be, se. to protect the innocent
- Results, needs further study:
 - *useless statistics*

Root zone file analysis

- Resource Records: 1859
 - 1 SOA record
 - 1 TXT record
- 255 TLDs
 - 1216 Name server (delegation) records
 - Example: NL. 172800 IN NS SUNIC.SUNET.SE.
 - 5 Records per tld
 - 641 Glue records
 - SUNIC.SUNET.SE. 172800 IN A 192.36.125.2
 - Less than 3 per tld

Root zone analysis (cont.)

- No. of root servers: 13
- TLDs sharing in root name servers
 - ARPA. 172800 IN NS A.ROOT-SERVERS.NET.

.	13
ARPA.	9
EDU.	9
GOV.	9
MIL.	5
SE.	1

TLDs with specific Name Servers

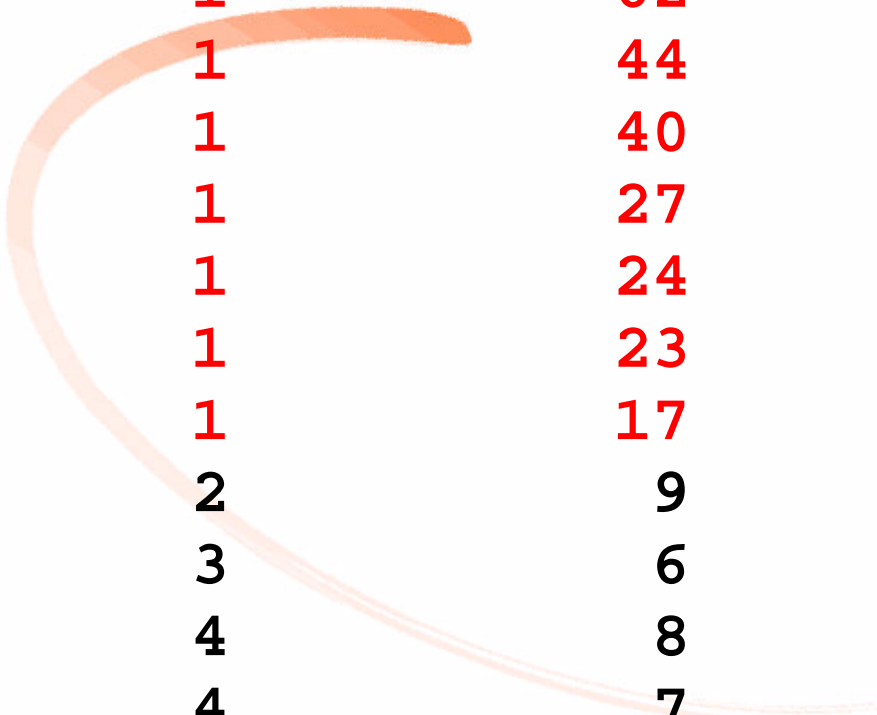
NL. 172800 IN NS SUNIC.SUNET.SE.

#TLD in #name servers

1	10
3	13
14	8
22	7
30	4
44	3
45	5
45	2
48	6

of Name Servers for TLDs

#NS serving #TLD



1	69
1	62
1	44
1	40
1	27
1	24
1	23
1	17
2	9
3	6
4	8
4	7
5	5
13	4
28	3
56	2
495	1

Closing Remarks

Supported by de. and nl.

- The packet switched internet network works
 - Control structure distributed by nature
 - Don't fix problems by adding central control
 - Strengthen the distributed control
- More risk analysis needed
 - Network level
 - DNS implementation



Questions?