DNSSEC – It's Still a Journey Until We Reach the Destination

Edward Lewis

Neustar

APRICOT 2009

Development of DNSSEC

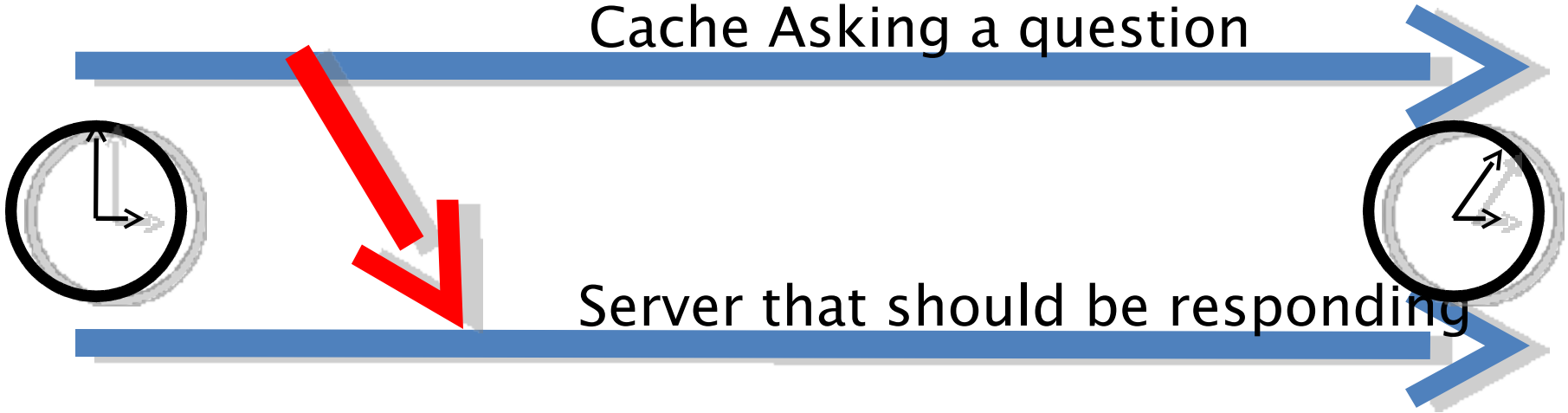
- For about 15 years interest and progress in DNSSEC has varied like waves on the ocean
- A year ago, at APRICOT 2008, DNSSEC was at a low point, it seemed unlikely to succeed
- Last summer something happened and now DNSSEC "buzz" is riding high
- But today DNSSEC is not prepared to be immediately deployed, despite past

Cache Poisoning

- DNSSEC began with a simple goal
  - Stop cache poisoning
- It did this by providing a signature
  - To tie the answer to the source
  - To demonstrate completeness
- Briefly, what is cache poisoning?
  - This underlies DNSSEC's popularity rises and falls

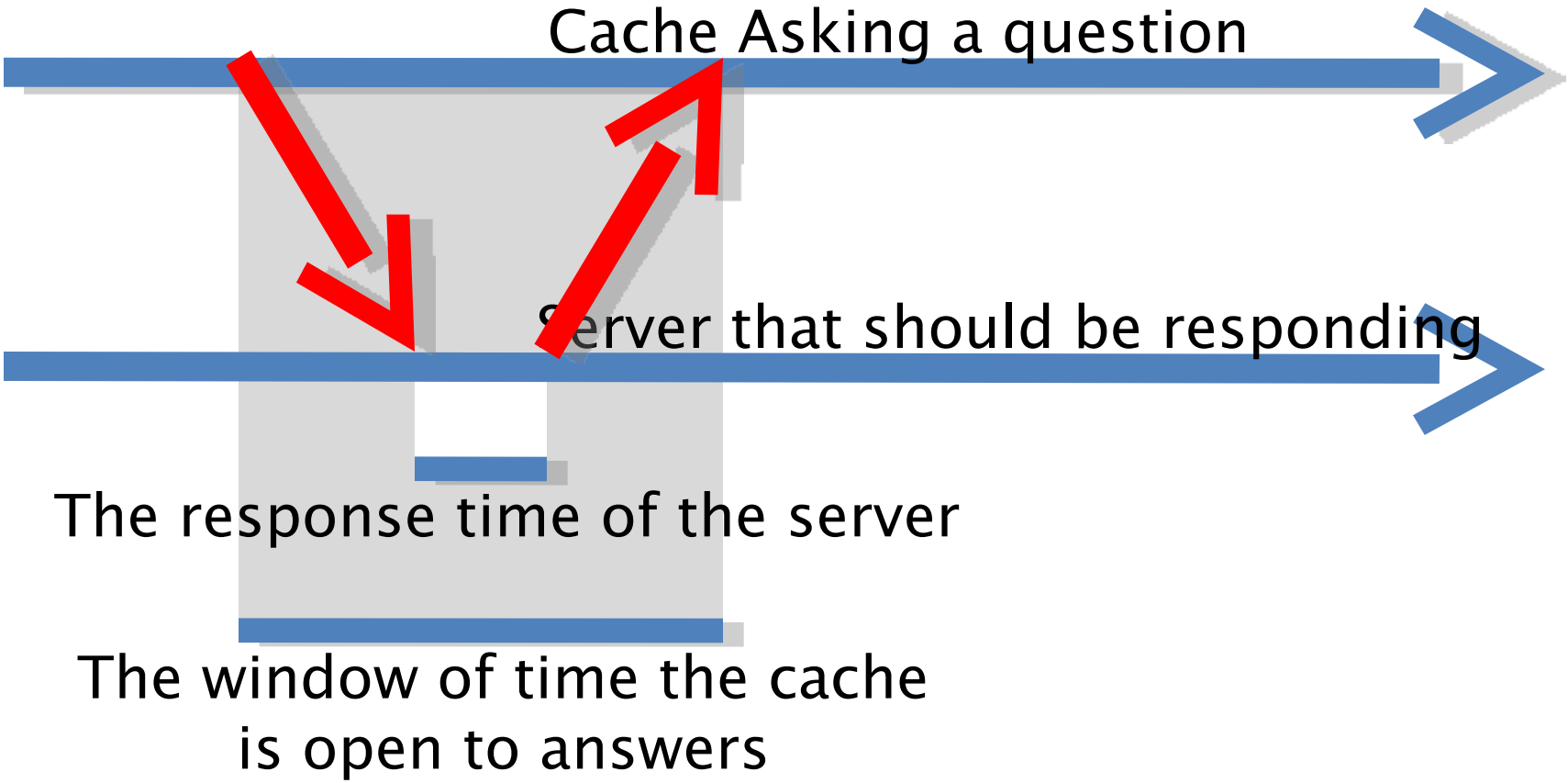
Query and Time

Using a graph showing time passing from left to right:



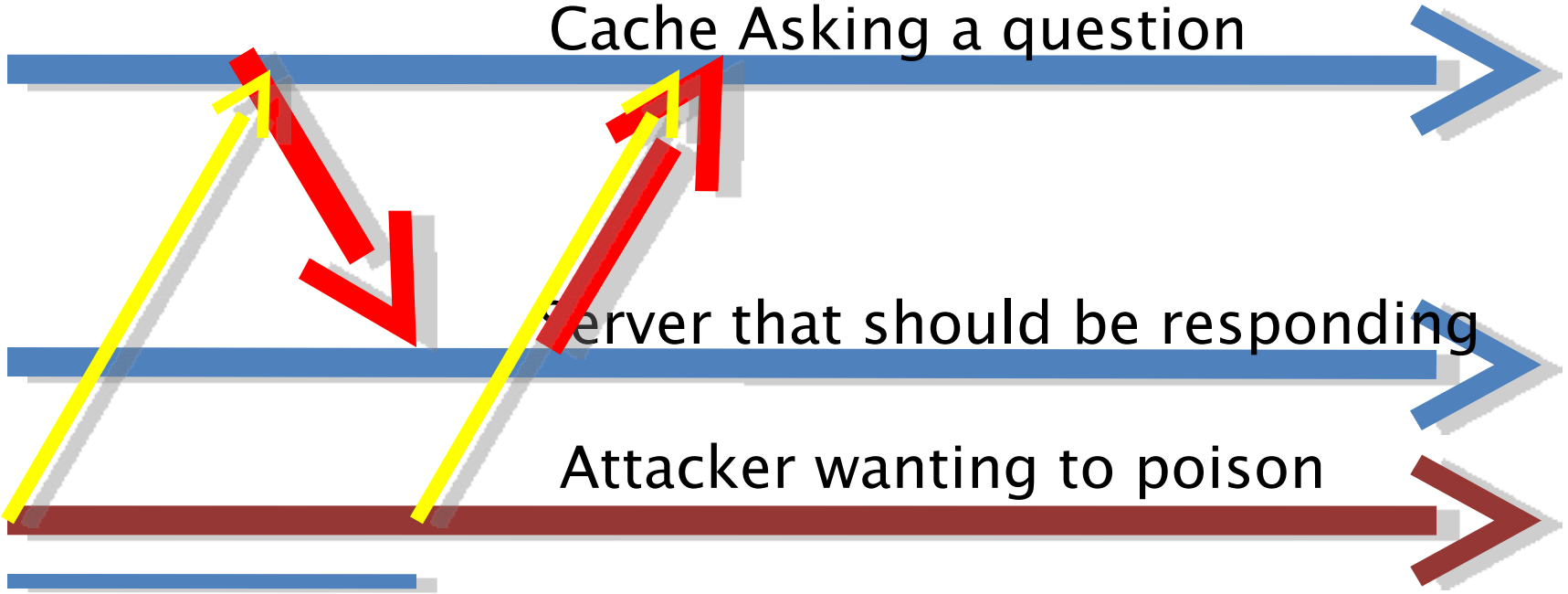
The angle shows that transmission of a message takes some time

Query, Response and Time



The Open Window

Using a graph showing time passing from left to right:



Attacker's window of "opportunity"
to poison the cache, same duration
but earlier in time

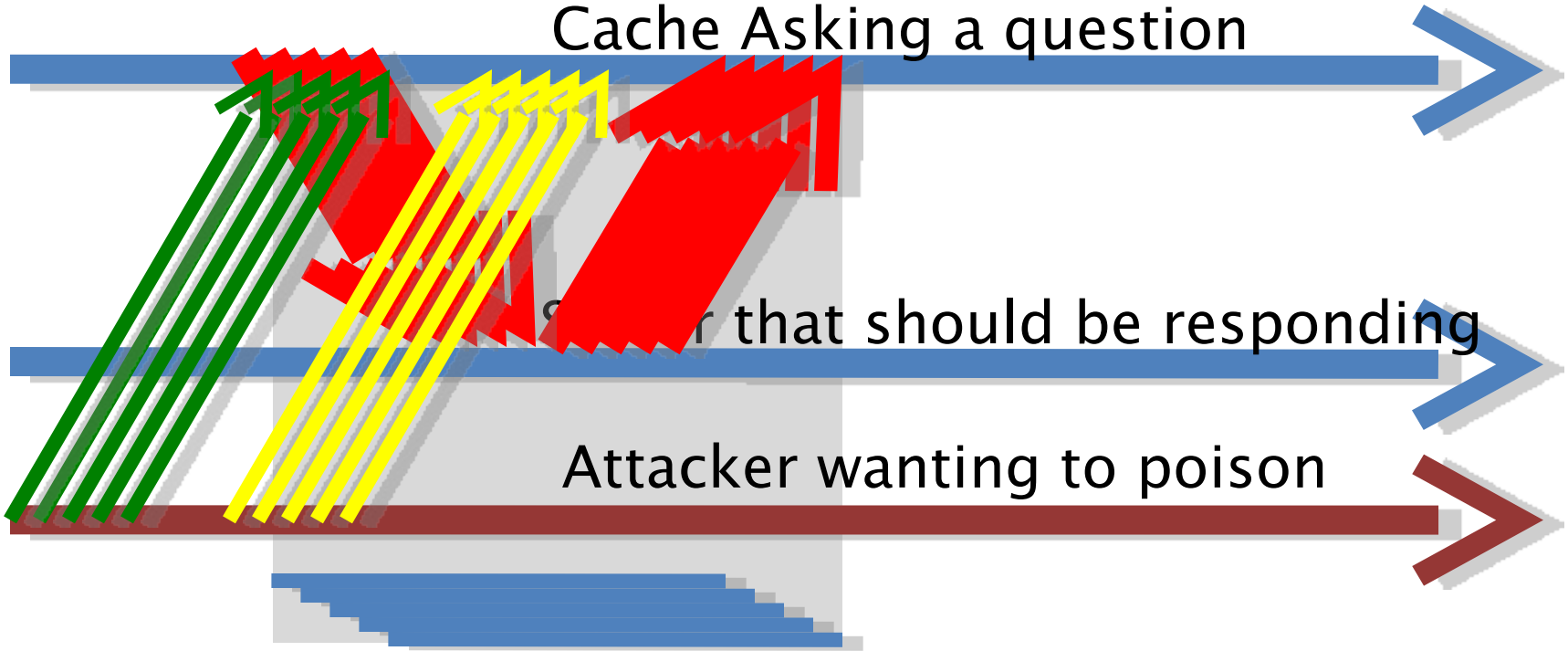
Inside the Window

- Cache is "picky" about accepting a response
- A lot of fields have to have the correct values
- The window is brief, somewhat unpredictable
- DNSSEC fell out of favor because
  - Caches became pickier as we fixed the protocol
  - Processing times made the windows

US-Cert VU800113

- Last year Dan Kaminsky discovered a way to bring cache poisoning back to life
  - by launching multiple, parallel queries
  - attacker determines when a window opens
  - attacker determines how many windows are open
  - this gives attacker a great chance of forging all the needed fields to get into cache

New Vulnerability



Attacker's window of "opportunity" is now "***windows***"

green = queries, yellow = poisoning attempts

Is DNSSEC ***now*** the answer?

- We are sure we need DNSSEC
  - No short cuts remain!
- Can't we just ignore the new (summer) threat?
  - Attacks are already a concern they are happening
- Can we "dodge" DNSSEC with something else?
  - Short term treatments, but no replacement

Where is the *SuperDNSSEC* hero?

- The superhero cape and tights not quite ready
  - Software and operations are largely untested
  - A significant element (NSEC3) is "barely" available
  - Few registries have experience with DNSSEC and those with - only with "early adopter" registrants
  - Operations and process for signing, registration, validation are mostly

Fitting the cape and tights

- Or, why is it *still* a journey to the destination?
  - We need to have a signed root, TLDs
    - It's only a start, still it is a "must"
  - We have to make sure the DNS supply chain elements are individually incented to deploy DNSSEC
    - Registration process (registrars), DNS service providers
  - We have to get the "end" players up and running

Past Deployment Focus

- Championing DNSSEC in recent years
  - Focus on registries, e.g., signing the root
  - Focus on end-user client tools
    - Web plug-ins to show DNSSEC in use
    - Tools to manage DNSSEC in simple zones
- Evidently, the problem is not just registries and tools
  - Or else we'd be done by now

DNS Supply Chain

- What is that?
  - Registrant, Registrar, Registry for start
  - DNS operator/service provider
  - ISPs running recursive servers
  - Domain retailers
  - Enterprise in-house IT department(s)
  - Specific to DNSSEC (Trust Anchor Repository)
  - Service integrators (a registrar that hosts, etc.)

Incent the DNS Supply Chain

- Fundamental rule: a (successful) change must do at least one of two things
  - Decrease cost of operations
  - Increase benefit of services
- DNSSEC costs need to be identified
- DNSSEC benefits recognized for each player
  - For some it is "clear", for others (registrars) not

Why is DNSSEC still a journey?

- Today we can't rely on DNSSEC protection
  - Don't have a signed root zone
  - Need to test, fit it into operations
  - Need a supply chain for DNSSEC data
- Could be looking at 12-18 ("X") months before we can rely on DNSSEC protection
  - Still some work to do yet
  - dotCOM "in 2011"

With DNSSEC "going forward"

- We have attacks happening every day
- What is being done now, pre-DNSSEC?
- A look at three offerings
  - Infoblox
  - Nominum
  - UltraDNS

Infoblox

- Offers a DNS Firewall product
- DNS Firewall product
  - http://www.infoblox.com/news/release.cfm?ID=129
  - Watches for suspicious traffic
  - Reports/raises alarms
- Please refer to that announcement for details

Nominum

- Employs a "Layered Defense" for a more hardened name server
  - http://www.nominum.com/download/Layered%20Defenses%20for%20DNS%20Security.pdf
- Layers
  - More difficult to spoof
  - Detection of attack
  - Glue management
  - Reporting

UltraDNS / NeuStar Plans

- Until summer, a patient stance on DNSSEC
  - "Cost versus benefit" balance now favors DNSSEC
- Support customers who are early adopters
  - Identifying ways to protect our customers sooner
- Immediate plans
  - Deploy a new service called

What Should You Do

- Make sure your DNS code is new
  - Consult this for list of vulnerable code
    - http://www.kb.cert.org/vuls/id/800113
  - If you use
    - BIND (https://www.isc.org/node/326)
    - Unbound (http://www.nlnetlabs.nl/publications/unbound_patch_announce.html)
- Consider an interim option
- Get ready for DNSSEC (it only takes 6 minutes)

End of Slides

- Open mic...

- Or, follow up questions can be sent to the address in the slide footer.