DNS Security

Paul V. Mockapetris
Chairman & Chief Scientist, Nominum
ENISA November 13, 2008

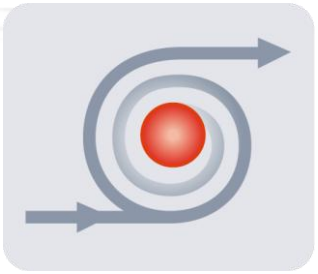
Introducing Nominum

Mission	Product Leadership	Technical Expertise	Strategic Partners
Delivering the Trusted Internet Experience ***FAST,*** ***RELIABLE,*** ***SAFE***	***Best Security*** ***Highest Performance*** ***Highest Scalability*** ***Guaranteed Availability*** ***Architecture for Services***	• ***Dr. Paul Mockapetris*** Inventor of DNS IETF Chair: 1994-1996 Lifetime award: ACM SIGCOMM 2005 • ***Bob Halley*** Co-Architect of BIND8 Architect of BIND9 • ***Ted Lemon*** Developer of ISC-DHCP Co-author of DHCP Handbook	Nokia Siemens Networks acme packet Sun microsystems InfoSpace Juniper Networks

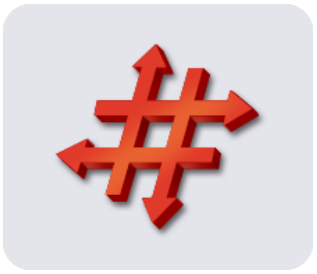
150 million+ broadband households served across 100+ leading service providers

Nominum Product Family

Advanced Servers



Vantio Suite
Advanced DNS Extensions
(Redirection Rules, Analytics)

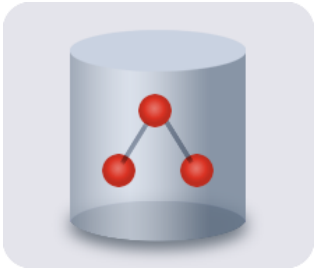


Navitas Suite
IP-application
Routing Directory

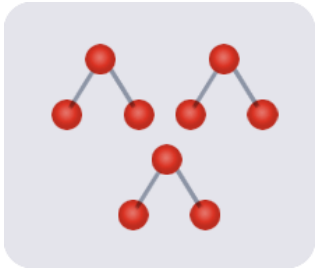
SML (Centris)
IP and Domain
Reputation Directory

Foundation Servers

DNS

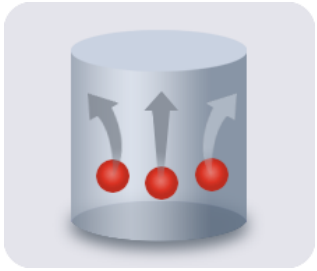


ANS
Authoritative
Name Server



CNS
Caching Name
Server

DHCP



DCS
Dynamic
Configuration
Server

Commercial-Grade Features

- Guaranteed availability
- Comprehensive easy-to-use interfaces
- Built-In Security
- Online maintenance
- Flexibility

Awards

2006 Internet Telephony Product of the Year

Fierce VoIP Winner 15

TechWorld

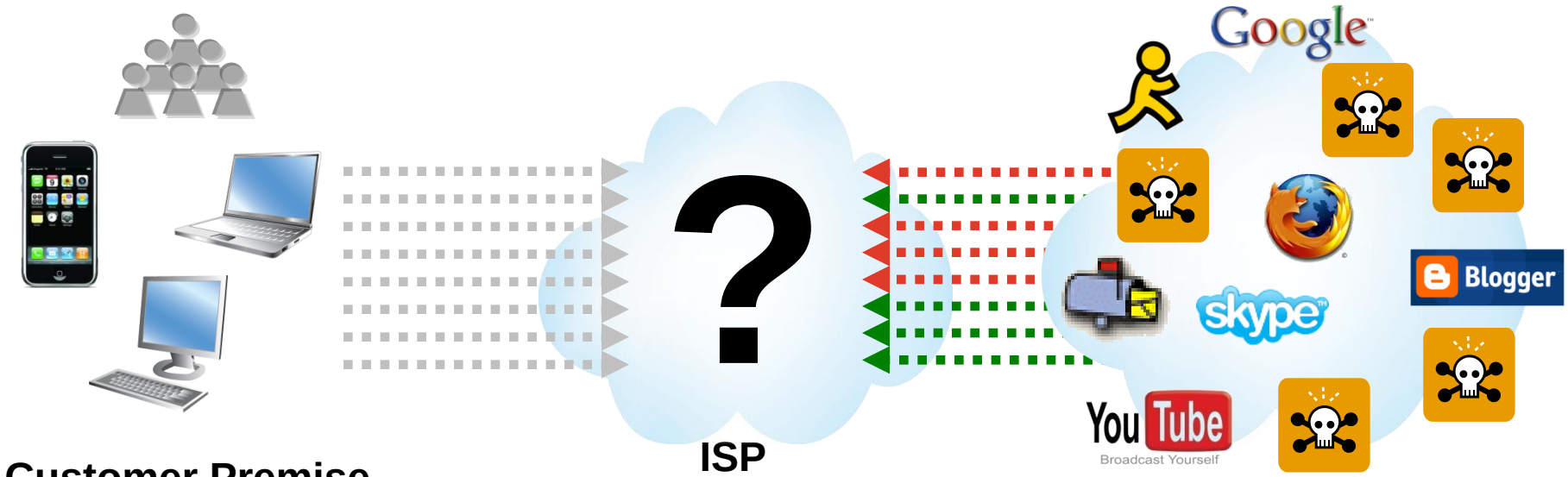
Internet Telephony Excellence Award

2006 Frost & Sullivan North American Product Innovation Award

pulver 100 Companies to Watch 2007

Rapidly Growing Problem

How to determine the difference between safe and harmful requests in real time?



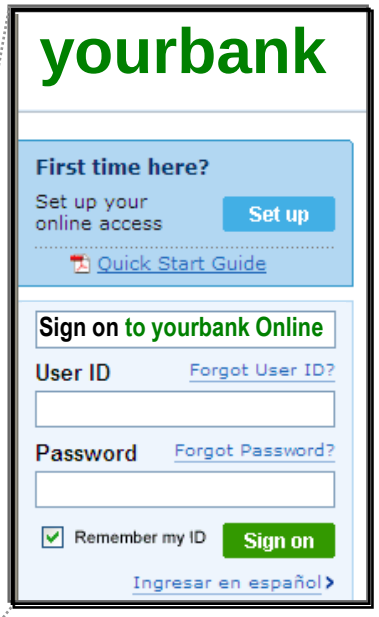
Customer Premise

ISP Broadband Network

Internet
150 *million* malicious hosts and growing…

How Can the Service Provider Help?

How do Computers Navigate the Network?

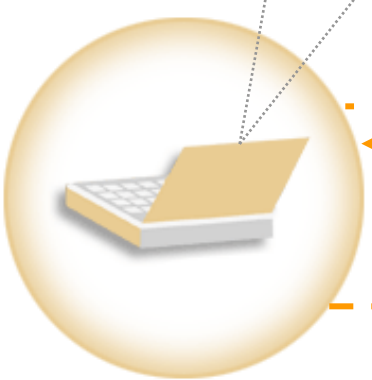


To get to www.yourbank.com, the computer asks its local name server for directions.
For a company, it's the company's DNS server.
For a broadband user, it's the ISP's.

ISP or Enterprise Caching DNS

How do I reach www.yourbank.com ?

www.yourbank.com Is at 1.2.3.4



User browsing

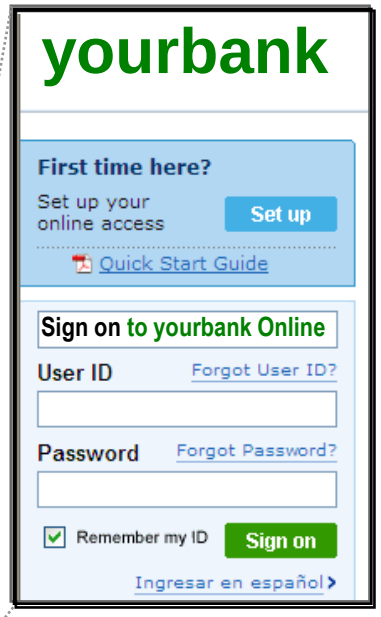
TCP Me to: 1.2.3.4

Internet

Your Bank

www.yourbank.com
1.2.3.4

Cache Poisoning Attack



Attack Server

www.yourbank.com
Is at 9.10.11.12

ISP or Enterprise Caching DNS

Hacker Bank

How do I reach www.yourbank.com ?

www.yourbank.com
Is at 9.10.11.12

www.yourbank.com
9.10.11.12

Your Bank

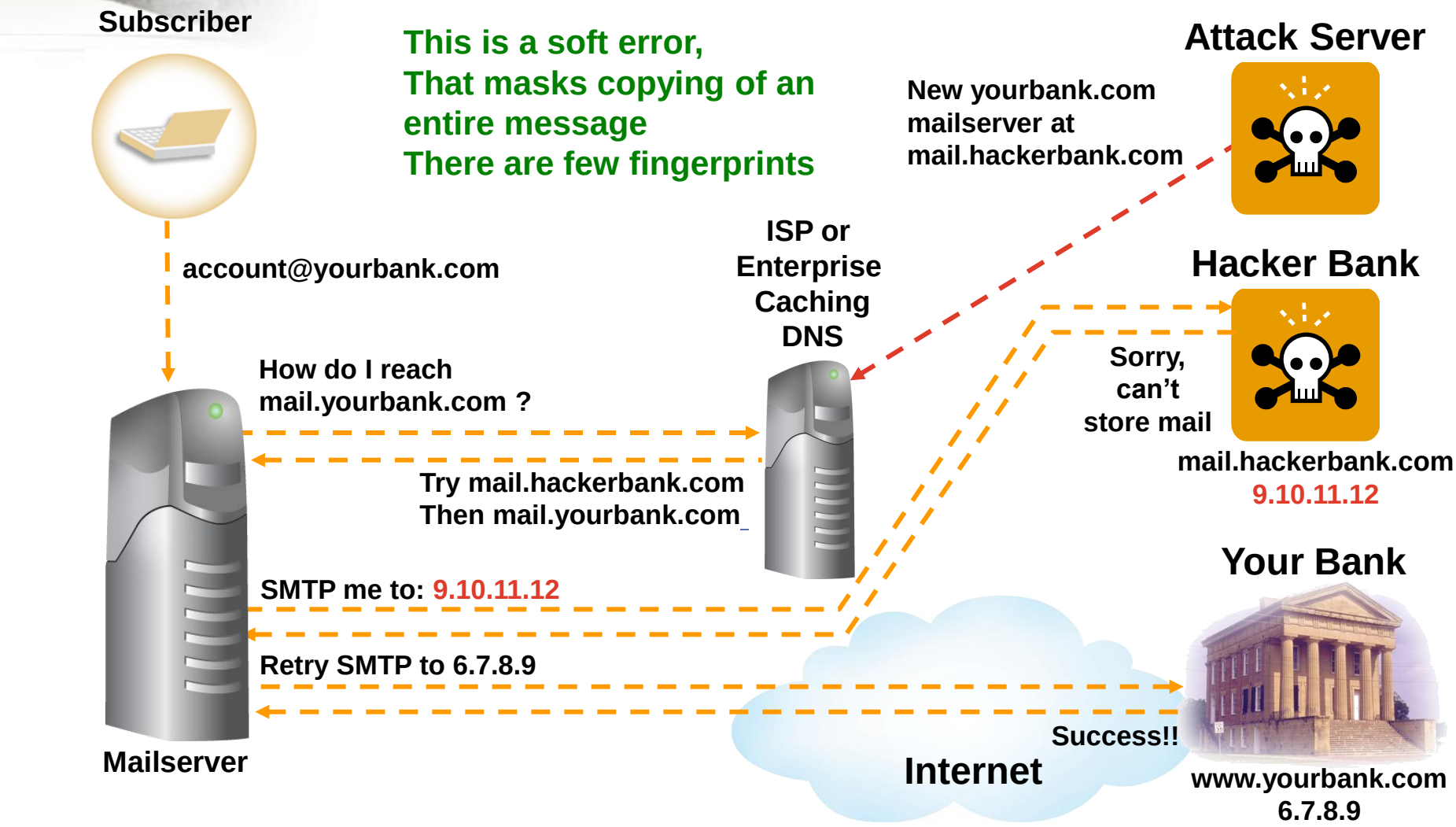
User browsing

TCP me to:
9.10.11.12

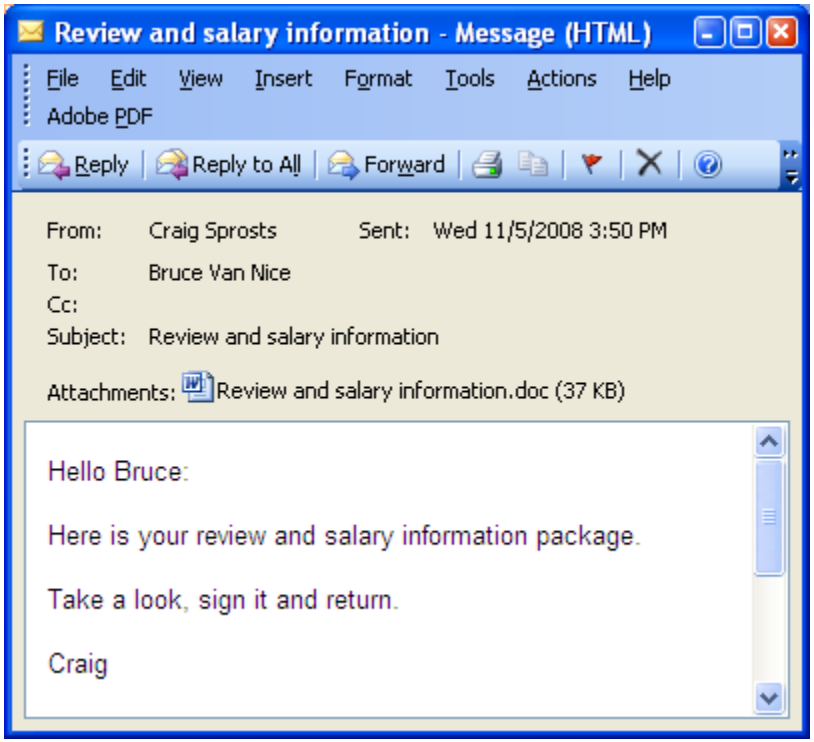
Internet

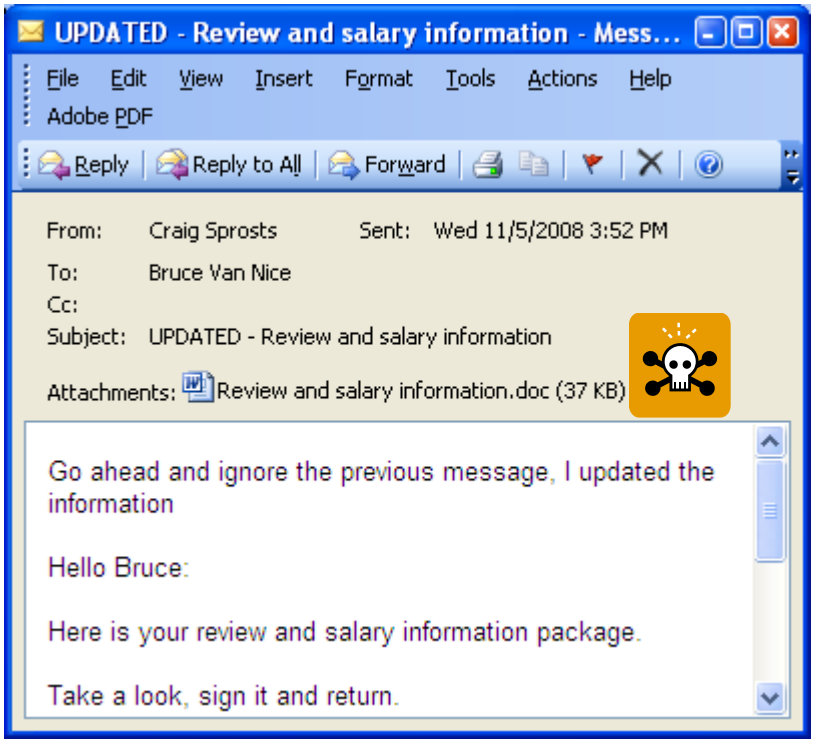
www.yourbank.com
1.2.3.4

Mail Attack


Subscriber
This is a soft error,
That masks copying of an
entire message
There are few fingerprints
Attack Server
New yourbank.com
mailserver at
mail.hackerbank.com
account@yourbank.com
ISP or
Enterprise
Caching
DNS
Hacker Bank
How do I reach
mail.yourbank.com ?
Sorry,
can't
store mail
Try mail.hackerbank.com
Then mail.yourbank.com
mail.hackerbank.com
9.10.11.12
Your Bank
SMTP me to: 9.10.11.12
Retry SMTP to 6.7.8.9
Success!!
Internet
Mailserver
www.yourbank.com
6.7.8.9

Two Messages





Fast Poisoning & Enterprise

- The higher speeds of enterprise networks make them especially vulnerable!
- Gigabit ethernet: 50% success after 5 hours
- Vectors
  - Infected laptops
  - Web content, email from the outside

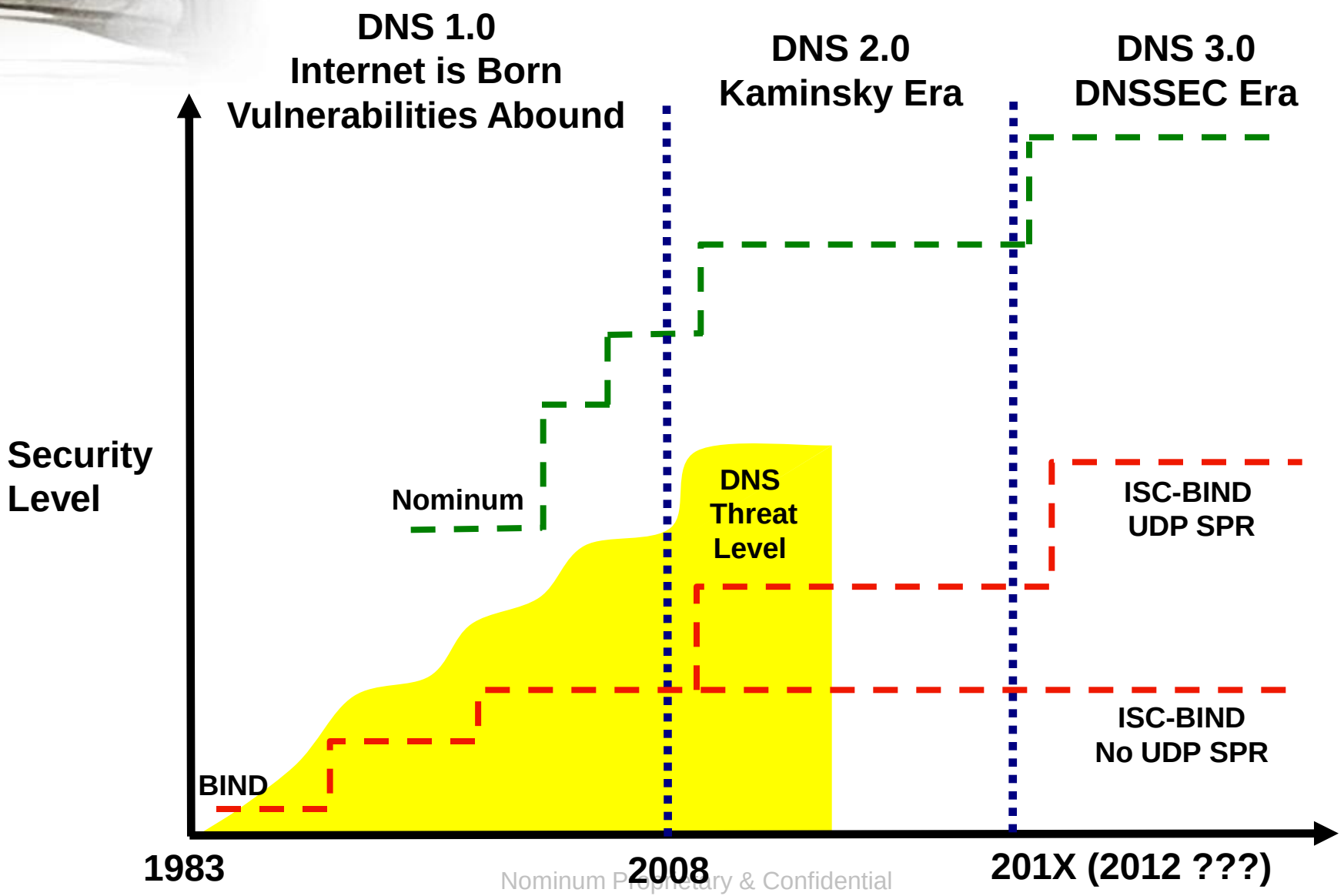
DNS Security History (past and future)

- 1983 DNS starts
  - » Intentional omissions include security
- 1986 DNS liftoff
- 1989 Cache Poisoning observed
  - » “Don’t cache data just because somebody sends it to you”
- 1989-2008 Various cache poisoning attacks
  - » Multiplexing technology adapted for security
  - » Other defenses deployed
- 1993 DNSSEC starts
- 2008 Kaminsky fast poisoning attack

…

- 201X Majority of DNS secured with digital signatures

A Changing World



DNSSEC Futures: What happens between 2008-201X?

Nominum.

I see three choices:

1. The current (?) DNSSEC version gets deployed
2. The current DNSSEC gets used, DNSSEC++ gets deployed
3. Some other security method for DNS gets deployed

Either 1 or 2 requires some "tough love" for DNSSEC or the $Billion attack

Essential “Tough Love”

- Distribute authority
- Simple administration
- Applications need help
- Understand the alternative

Distribute authority

Broken Theory #1:

"In the ideal situation you have only one key configured as a secure entry point"

- ICANN doesn't need a monopoly on signing the root key, you could just have it and others distribute TLD key set via DLV or a similar mechanism

- It's just an unrealistic way of thinking about security

Simple administration

Nominum.

Broken Theory #2:

"You should build tools to maintain your signed zones e.g.: using `cron`, `perl`, and `make`."

- We need a standard profile and set of tools that's understandable by a mere mortal.

- That is, a "zero geek" solution

Applications need help

Broken Theory #3:

The idea that only the resolver needs to be modified.

- In 1983, when we started the DNS, we spent a lot of time changing applications to deal with “Can’t find out now” answers.
- DNSSEC is harder. “Can verify” vs “can’t”, “clearly bogus” vs “poorly maintained”

Understand the Alternative

Nominum.

- The alternative will be encrypted paths between DNS servers.
- Maybe that's not so bad for the "legitimate needs of law enforcement"
- We will still be vulnerable to the whims of the sysadmins.
- We won't have a reliable infrastructure for new applications.

What can Service Providers Do?

Nothing

Common Ground

Need for a Trusted Internet Experience

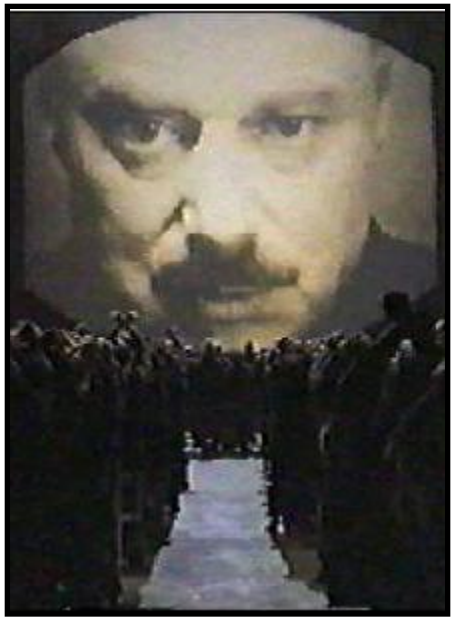
Stakeholders

- Subscribers
- Service providers
- Content providers
- Government
- Vendors

Issues

- Privacy
- Economic viability
- Technical viability
- Fairness
- User acceptance

Big Brother



The TRUE Thesis

- Protect the DNS, so it can protect you:
  - Secure existing DNS data
  - Use the DNS to collect, process, and distribute reputation data to enforcement devices:
    - Spam filtering
    - Firewalls
    - Caching DNS servers
    - DSL and cable boxes
  - Subset in production today; Internet Safety Alliance

- Use the world's largest distributed database to attack the Internet's biggest problem.

Beyond Today's True

- User-Selected reputation delivery
  - To the PC
  - To the DSL/Cable box
- Digital signatures for DNS a requirement

A more trusted and pure Internet experience