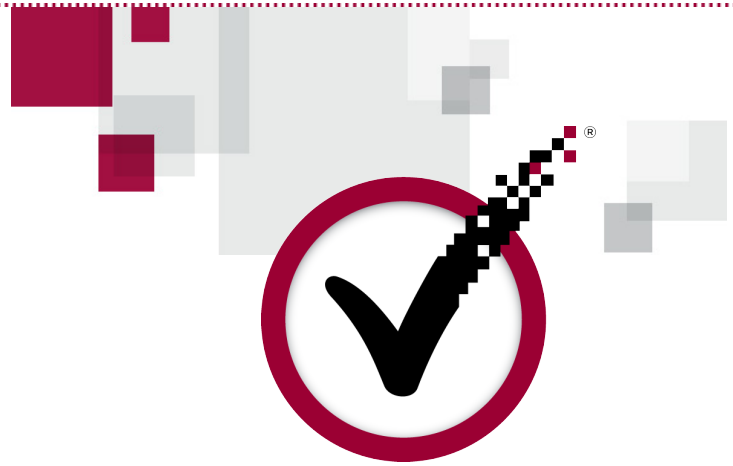
VeriSign®



The Evolving Nature of Internet Threats

Danny McPherson
Vice President, Research & Development
VeriSign, Inc.

Agenda

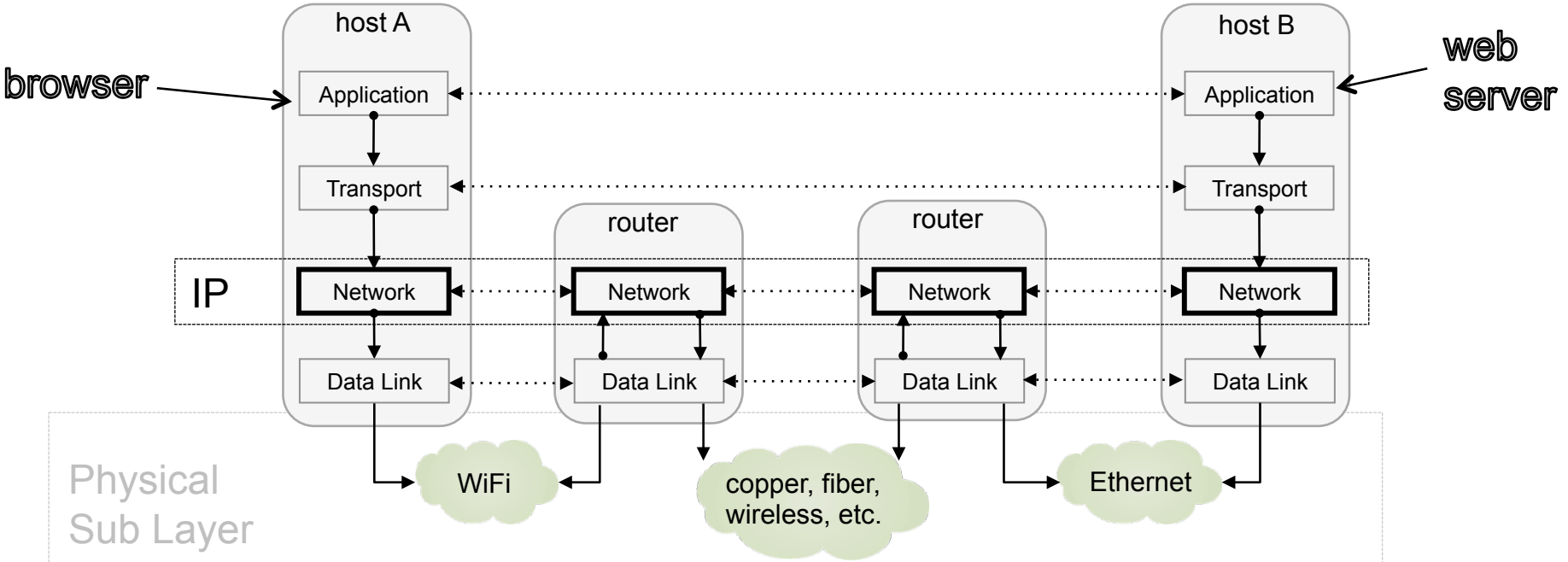
- IP and Internet Architecture Primer
- IPv4 Depletion and IPv6 Exhaustion
- Routing Security and Resource PKI
- DNS, DNSSEC and DNS Attack Surface
- Internet Security & Threat Landscape
- Wrap

The Internet Architecture

- Ubiquitous data communications platform; no single authority
  - Global collection of loosely interconnected networks
  - Datagram or packet-based connectionless network service
  - Ultimate goal is resilient **end-to-end any-to-any** connectivity
- Primary Internet Infrastructure Elements
  - Name: What we seek (DNS)
  - Address: Where it is (IP)
  - Route: How to get there (BGP)

- Security primitives enable
  - Systemic and wide-scale OR topologically localized attacks
  - Asymmetric threats
  - Complexity in attribution

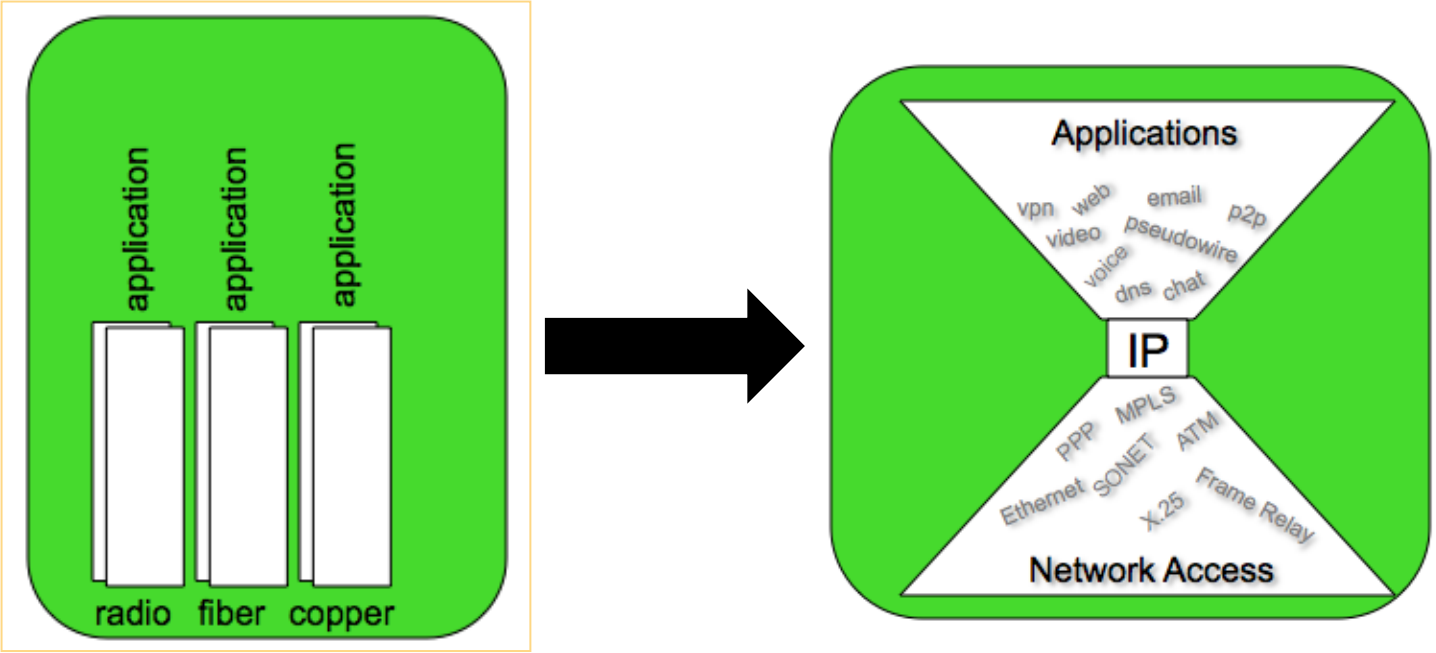
The Internet Protocol Model



- The IP model employs an **end-to-end** layered architecture
  - Transactions split into functional layers – IP @ "Network" Layer
  - Only IP and higher layers operate end-to-end – simplifies network devices
- Packets switched hop-by-hop based on destination IP address
  - Each device connected to the Internet requires a unique IP address
  - There are 2^{32} (4,294,967,296) unique IP addresses in IPv4

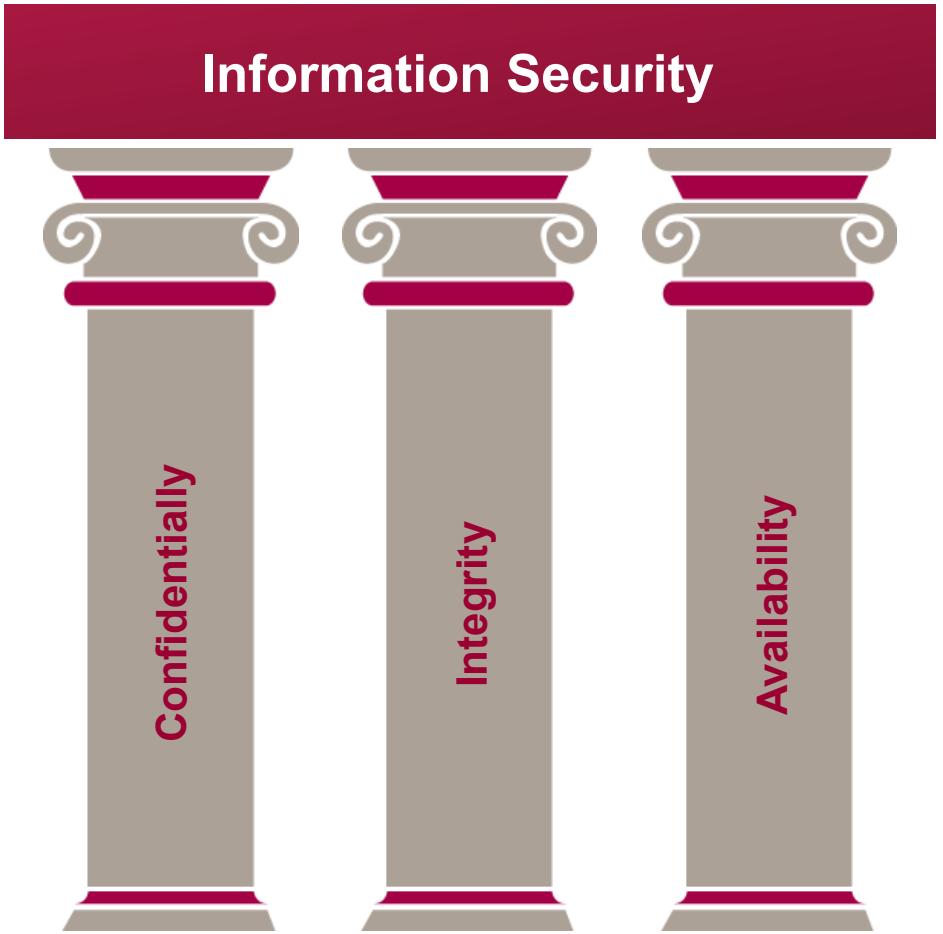
IP over Everything over IP

- ***Stovepipe*** architectures converge to common IP substrate
- IP ***thin waist*** of data communications – ***hourglass model***
  - IP must emulate essential attributes of native services
  - Converged services inherit IP attack surface

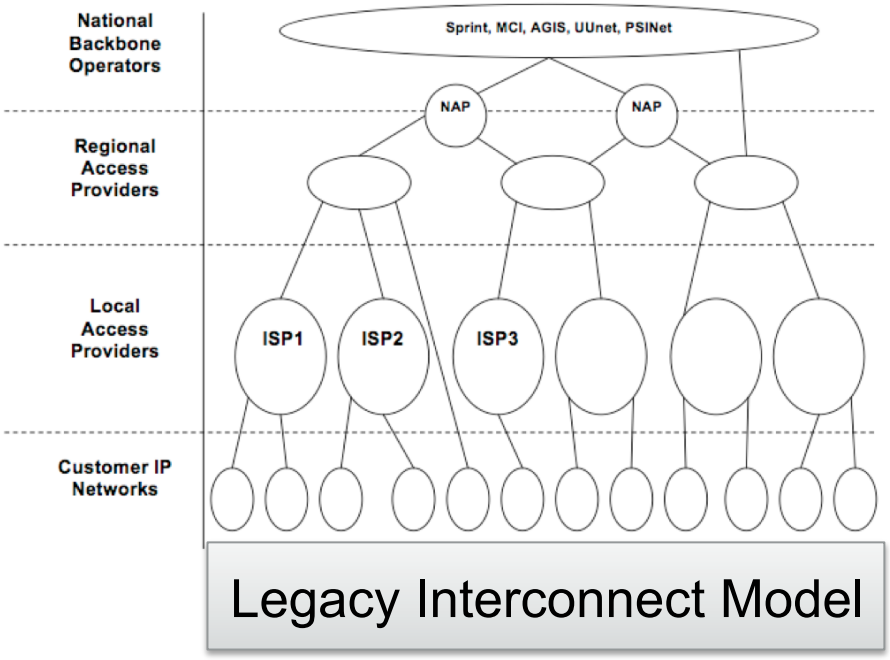


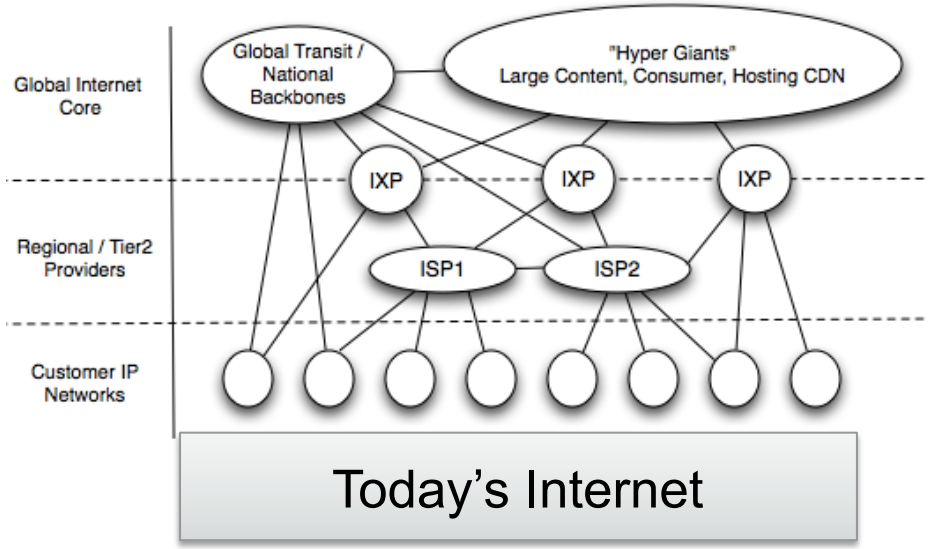
Three Pillars of Information Security

- **Confidentiality**
  - Is it secret, encrypted (e.g., PII)?
- **Integrity**
  - Is it authentic and accurate?
- **Availability**
  - Is it accessible with acceptable performance?
  - The forgotten pillar?



A Flatter Internet…

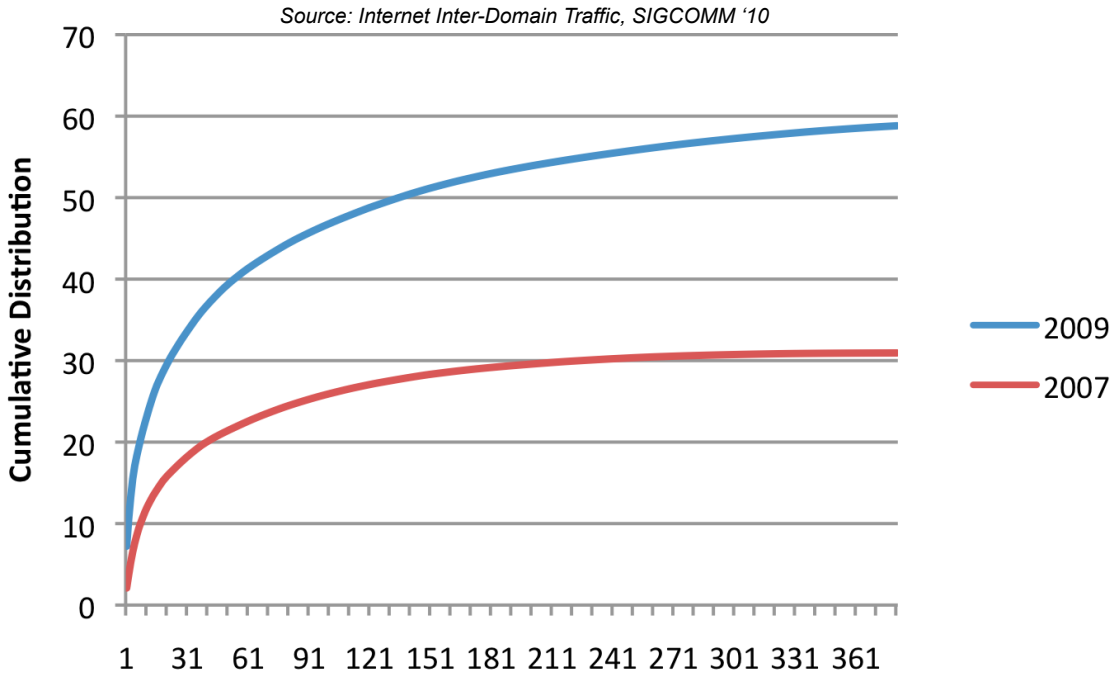




Order of magnitude growth, while mean AS topology 'distance' actually decreased

- Flatter and much more densely Interconnected Internet
  - Adds robustness & resiliency, ability to localize transactions
  - Presents routing, traffic, security & economic implications
- Disintermediation between content & eyeballs
  - New commercial models between content, consumer & transit networks

However :: Consolidation of Content

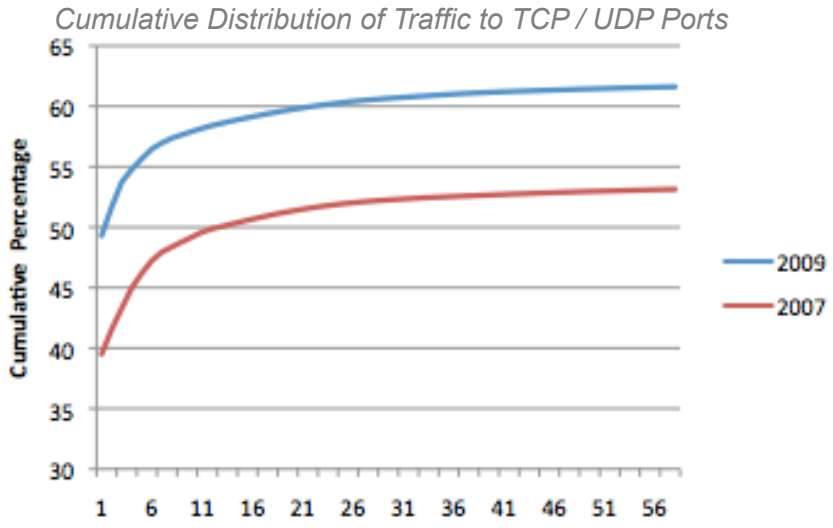


Rank	'09 Top Ten	%
1	*ISP A*	9.41
2	*ISP B*	5.7
3	Google	5.2
4	-	
5	-	
6	Comcast	3.12
7	-	
8	-	
9	-	
10	-	

Source: Internet Inter-Domain Traffic, SIGCOMM '10

- Content Consolidation
  - In 2007, thousands of ASNs contributed 50% of content
  - In 2009, 150 ASNs contribute 50% of all Internet traffic
  - 30 of ~150 'hyper-giants' contribute disproportionate 30% of all traffic
- Many shared dependencies emerge from economies of scale

And About End-to-End….

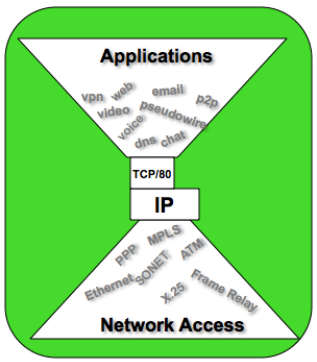


Source: Internet Inter-Domain Traffic, SIGCOMM '10

Rank	Application	2007	2009	Change
1	**Web**	41.68%	52.00%	**24.76%**
2	**Video**	1.58%	2.64%	**67.09%**
3	**VPN**	1.04%	1.41%	**35.58%**
4	**Email**	1.41%	1.38%	**-2.13%**
5	**News**	1.75%	0.97%	**-44.57%**
6	**P2P** (*)	2.96%	0.85%	**-71.28%**
7	**Games**	0.38%	0.49%	**28.95%**
8	**SSH**	0.19%	0.28%	**47.37%**
9	**DNS**	0.20%	0.17%	**-15.00%**
10	**FTP**	0.21%	0.14%	**-33.33%**
	Other	2.56%	2.67%	**4.30%**
	Unclassified	46.03%	37.00%	**-19.62%**

(*) 2009 P2P Value based on 18% Payload Inspection
Weighted average percentage of all Internet traffic using well-known ports

- Growing dominance of ***web*** as application front-end; concentration of application traffic over a decreasing number of TCP / UDP ports
  - Especially port 80, video
- Alleviate burden of ubiquitous network layer security policies
  - e.g., {permit tcp/80, deny *}
  - block auto-propagating worms and out-of-box services
- Demise of IP End-to-End?

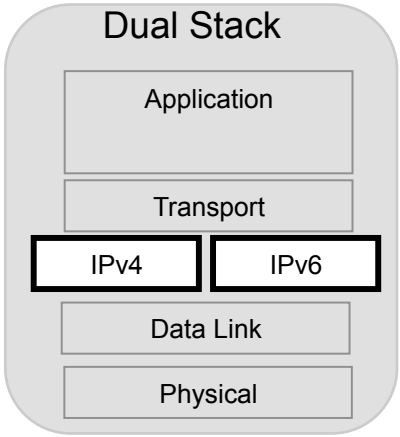


IPv4 Address Depletion and IPv6

- Internet growth has exceeded all expectations
  - IPv4 address space will deplete within the next year (~5.45% remains)
  - IPv4 depletion is not a new problem, first discussed in 1990
  - Initial estimates projected IPv4 depletion circa 2000
- The Internet community responded, developing several solutions
  - Removed “fixed size” classes/boundaries in IP architecture (CIDR)
  - Address sharing at the edge via network address translators (NATs)
  - Responsible IPv4 allocation policies and conservation efforts (RIRs)
  - Next generation IP design began early ‘90s, IPv6 finalized in 1999
- IPv6 provides 3.4×10^{38} addresses (340,282,366,920,938,463,463,374,607,431,768,211,456)
  - Not intended to be radical solution – considered conservative engineering
  - Used and managed similar to IPv4
    - IPv6 colon-separated hexadecimal address: **2001:1890:1112:1::20**
    - As opposed to IPv4s dotted-quad: **64.170.98.32**

IPv6 and Transitional Coexistence

- IPv4 -> IPv6 transition plan was '**dual stack**'
  - Both operate at Network layer, are not **'bits on the wire'** compatible
  - Transition plan best when plentiful quantities of IPv4 and IPv6 exist
  - IPv4 depletion will impair dual stack transition plan, introducing expense and potential disruption to Internet as service platform
  - Following depletion dual stack transition problems progressively worse



- Interoperability and Coexistence
  - Y2K had flag day, find all 2-digit 'year' data - change to 4
  - **Everything** in the IP stack has to handle either – or both
    - IPv4 devices may never be upgraded to IPv6
    - IPv6-only devices may need to communicate with IPv4 devices
  - Greenfield now with Large-scale/Carrier-grade NATS

IPv4 Exhaustion and IPv6 Deployment

- Wouldn't be an issue except there's no '*bits on the wire*' compatibility between IPv4 & IPv6
  - *Dual-stack* original (circa '96) IPv6 transition mechanism
  - No deployment incentive at the time (i.e., plenty of IPv4)
- No standard for IPv4 <> IPv6 protocol translation (e.g., NAT-PT historic)
- Zone contents increase as AAAA IPv6 DNS records are added
- Query rates increase as end systems are IPv6-enabled
- IPv6 preferences in host DNS resolution cause brokenness
  - Use AAAA if active v6 interface
  - Whitelisting by eyeball AND content networks fragment namespace
- Visibility to detect and mitigate IPv6 attacks requires new infrastructure capabilities (e.g., NetFlow extensions, ALG functions)
- IPv6 will impact all network, systems and networked application elements; needs explicit assessment – express executive level sponsorship and IPv6 preparedness planning should be well underway, within budget cycles

IP Addresses and the Future…

- IPv4 depletion is nearing, right on schedule -- just as predicted(!)

- IPv6 is necessary to remove the constraints we've been engineering around for approaching two decades now, and to unbridle innovation, new applications, and continued global Internet growth

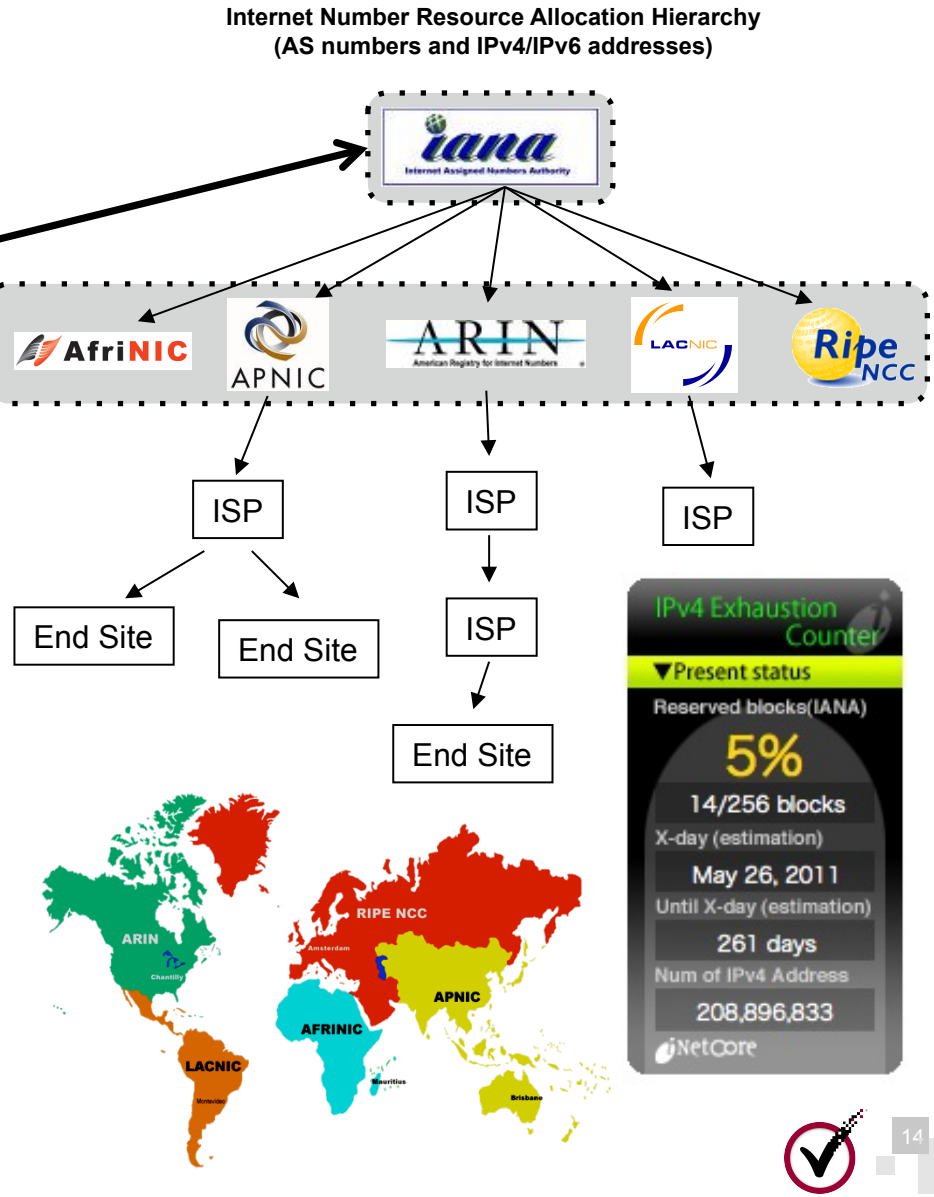
- IPv6 readiness planning is imperative; within budgeting and operational deployment cycles

IPv4 Fee Pool Exhaustion

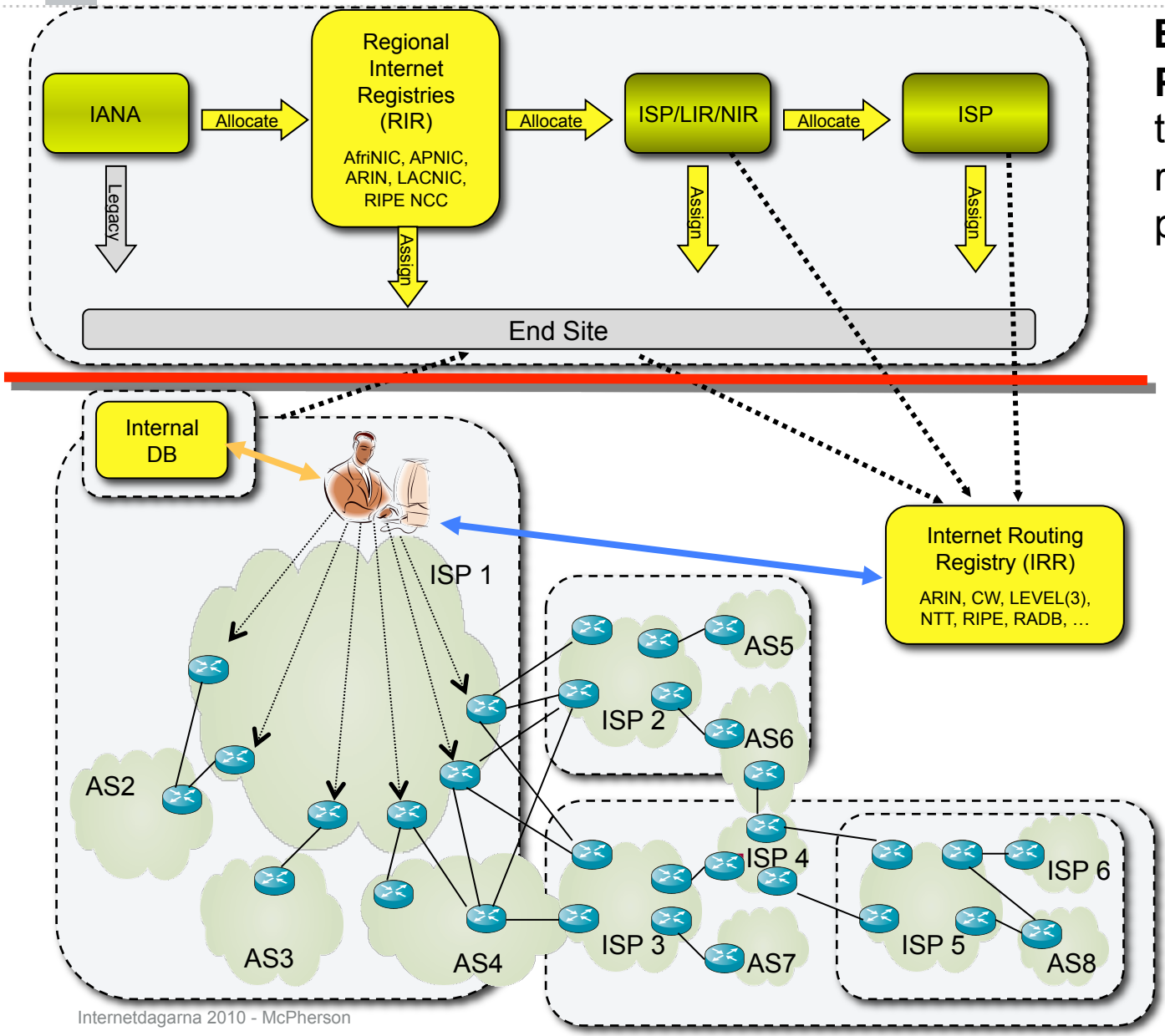
- Projected IPv4 free pool exhaustion within operational budgeting cycles (based on current rates)
  - IANA unallocated IPv4 pool exhaustion: **26 MAY 2011**
  - RIR unallocated IPv4 pool exhaustion: **25 JAN 2012**

  Source: http://www.potaroo.net/tools/ipv4/

- NO formally verifiable source exists to determine who holds what number resources
  - Absent this you can't secure inter-domain routing (BGP); requires
    - ***origin authorization &&***
    - ***path validation***



Internet Routing == 'Routing by Rumor'…



Border Gateway Protocol (BGP) used to advertise destination reachability (routes) to peers

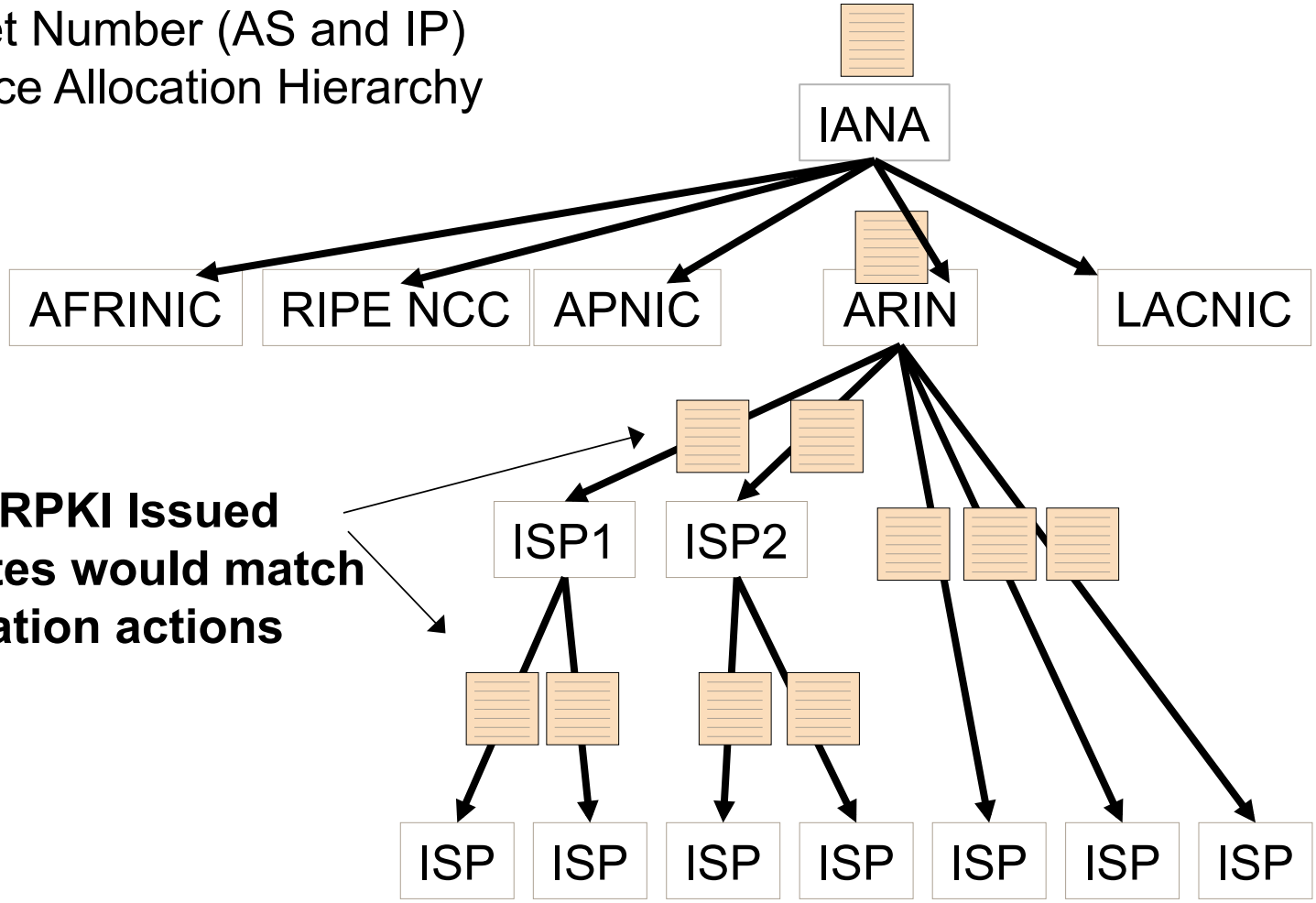
- Peers autonomously choose to reject, accept, and/or propagate routes
- No functional tie-in from resource allocation to routing system; no central arbiter
- ~50 IRRs; may or may not be used
- Little or no route filtering between ISPs today

Balancing Autonomy and Security..

- Today RIRs have no control (no operational role) over the number resources they're charged with managing
  - **Black Market** for IPv4 address space **already** exists
  - IPv4 exhaustion (IANA < 12 months, RIRs shortly thereafter)
  - IPv6 **not** 'bits on wire' compatible with IPv4; complex translations, hefty middleboxes required (e.g., ALG, DNS AAAA <> A synthesis, NAT-PT, state-based, lost transparency, etc..)
  - Result: IPv4 Black Market expands
- Alas… RIRs now have incentive to build Resource PKI (RPKI)
  - Registries become ***title agents***; not allocators
  - IF RPKI employed for routing policy provisioning, autonomy that exists today must be balanced with hierarchy and security through RPKI
  - Third party now involved in routing; expanded operational elements
- **If you think DNSSEC politics are complex..**

Resource Certificates

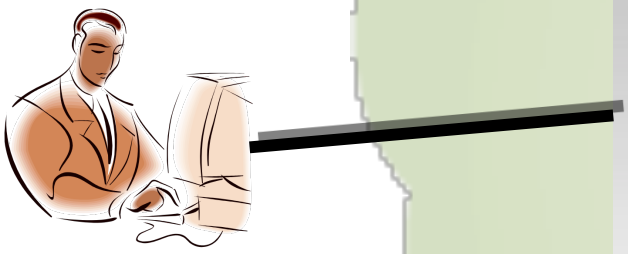
Internet Number (AS and IP)
Resource Allocation Hierarchy



With RPKI Issued Certificates would match allocation actions

Informing routing policy simply one application of resource certification

The Internet…

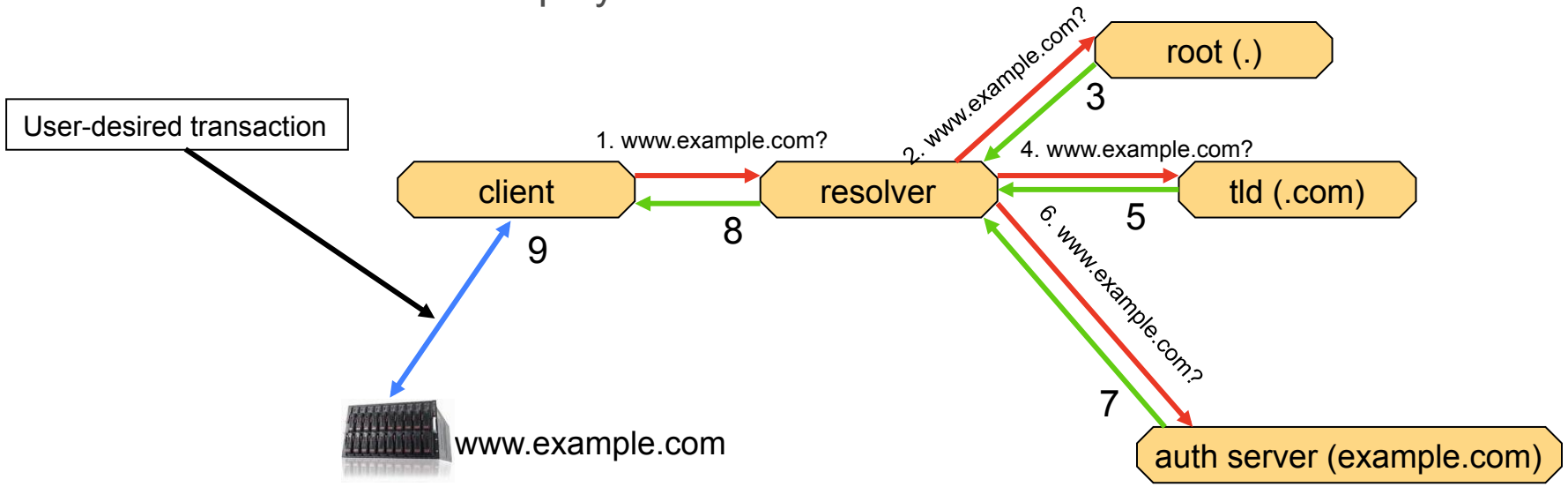


Average user or digital immigrant?

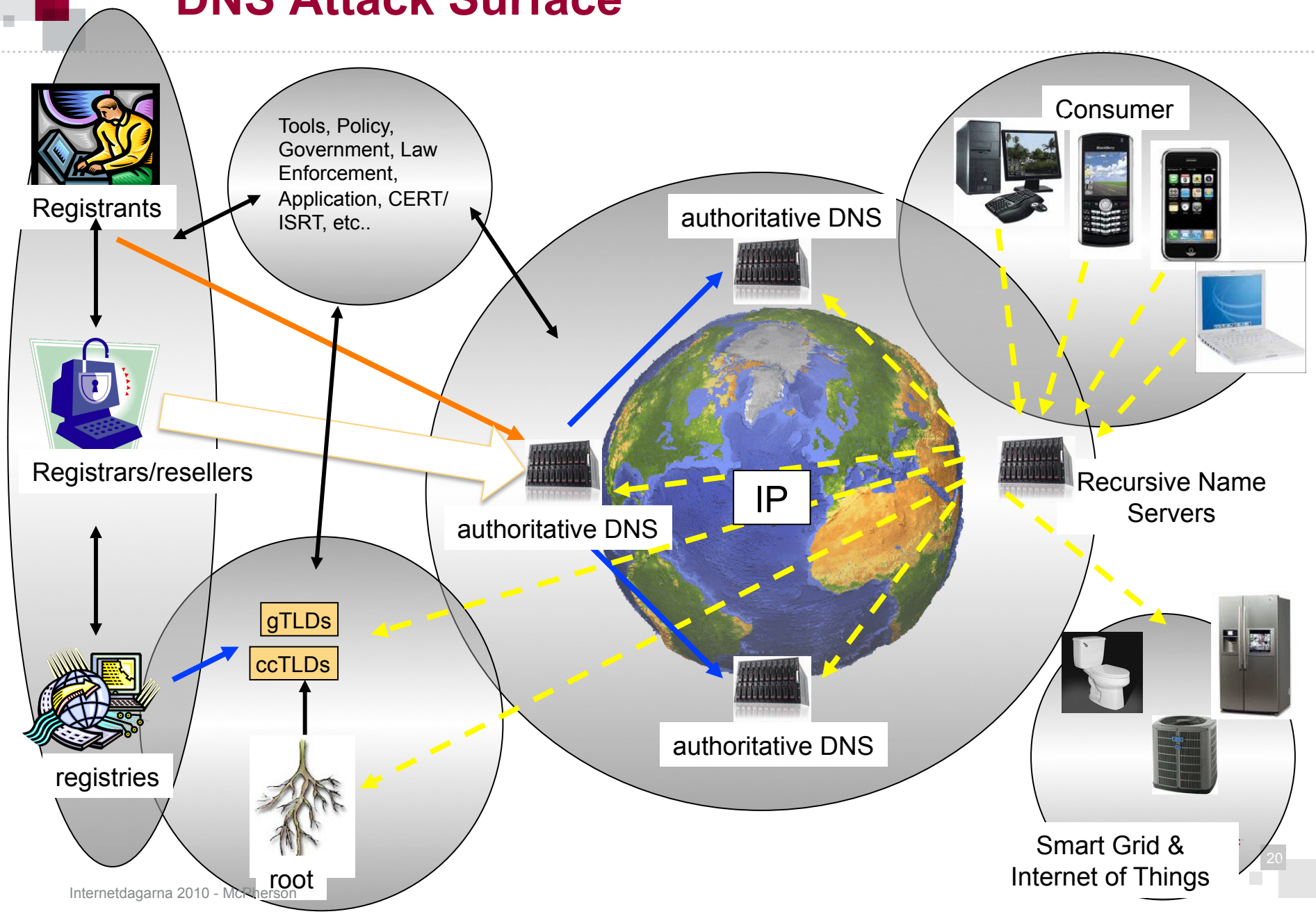
Most users consider the Internet is a big disk drive on the other end of their broadband connection – they don't realize the variables involved in a transaction

What's DNS?

- Domain Name System - Maps {key,type} tuples to set of unordered values
  - E.g., human-readable names (e.g., www.example.com) to machine-usable numbers (i.e., IP addresses; 192.168.100.1)
- 'Under the covers' and simplicity of use leads most folks to underestimate the complexity of the DNS
  - until broken or employed for malice



DNS Attack Surface



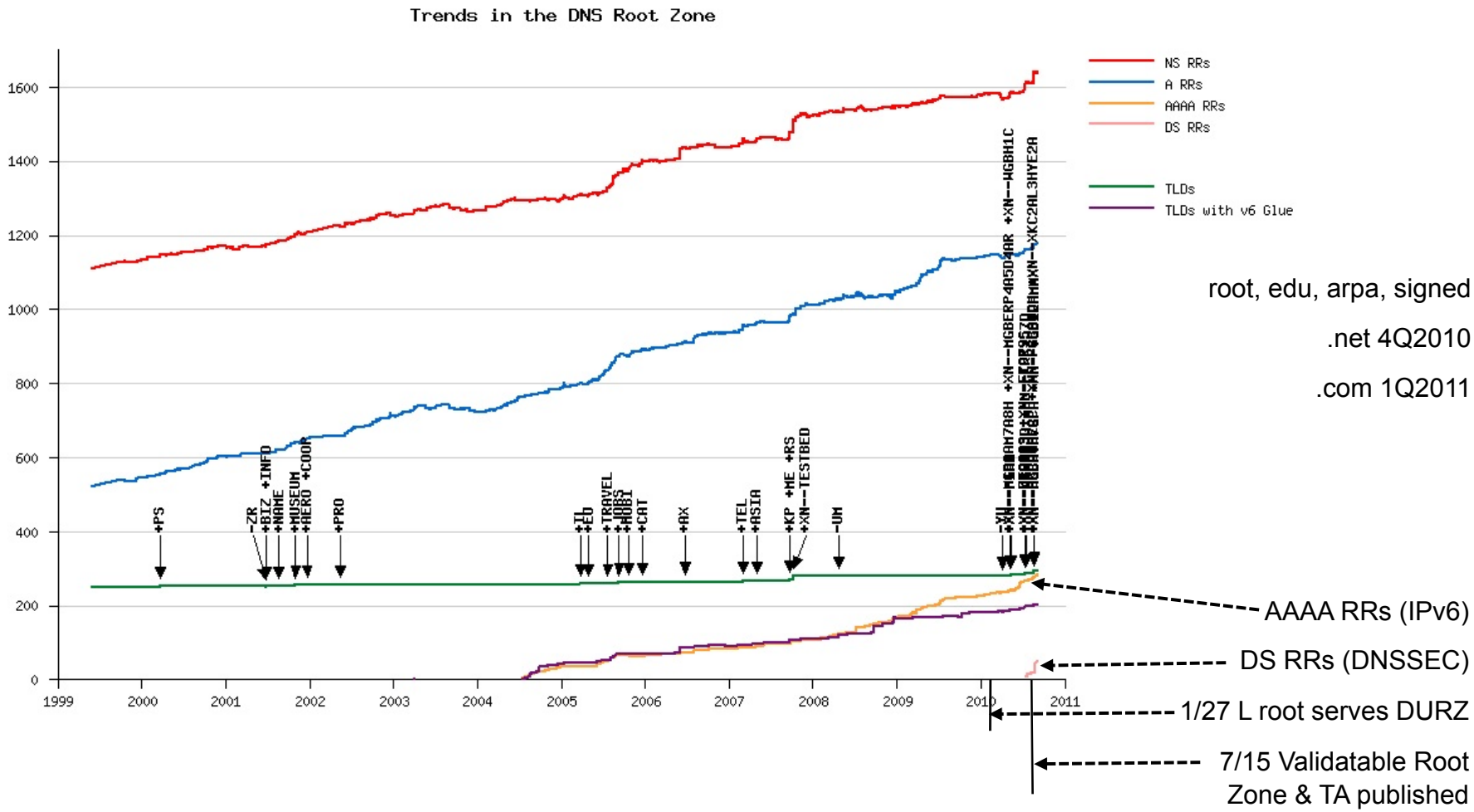
DNS is 'Multi-tenant'

- Hierarchal nature of DNS renders inherent multi-tenancy
  - massive root and TLD transaction capacity absorbs and topologically localizes most volumetric attacks; attackers usually look elsewhere
- Domain name registrar bundling, economies of scale, and niche managed DNS services players
  - Yield natural high-density clusters of authority service operators
  - DDoS on single target domain often results in collateral damage for hundreds, or thousands, or more(!) domains
  - more tenants == higher attack probability(?)
- Zone compromise via key loggers or phishing for registrant's registrar and managed DNS administrative interface credentials
  - Very common point of attack
- Misbehaving or malicious applications often overwhelm regional recursive name servers, commonly triggering cascading resolution failures

Growth in Complexity Of DNS

- DNSSEC zone management, transaction overhead, key rollover, recursive name server state and systemic complexity expand as more zones are signed and validation increases
- IPv6 will drive growth for AAAA records and dual-stack hosts, expect increased aggregate DNS transaction rate as much as ~2x during extended IPv4/IPv6 transitional co-existence (parallel or iterative A & AAAA queries) – transport and content implications
- IDNs and i18n increase root and TLD size and combinatorial variables, drive localization and complexity in applications, introduce new security issues
- Applications optimize for client interactivity & demographics, increases systemic churn, query frequency, pre-fetching, TTLs, etc. (e.g., CDNs, Google's 'instant search', etc.)
- Multi-homed end systems (e.g., smartphone w/Bluetooth, 802.11 & 3G), application-level resolvers and validation, etc.. drive more queries, introduce split DNS, policy implications

Root Zone Trends



Currently ~294 zones in root, ~40 corresponding DS records, and ~293 AAAA records

Uptick in new RR types and associated complexity considerable

DNSSEC Adoption

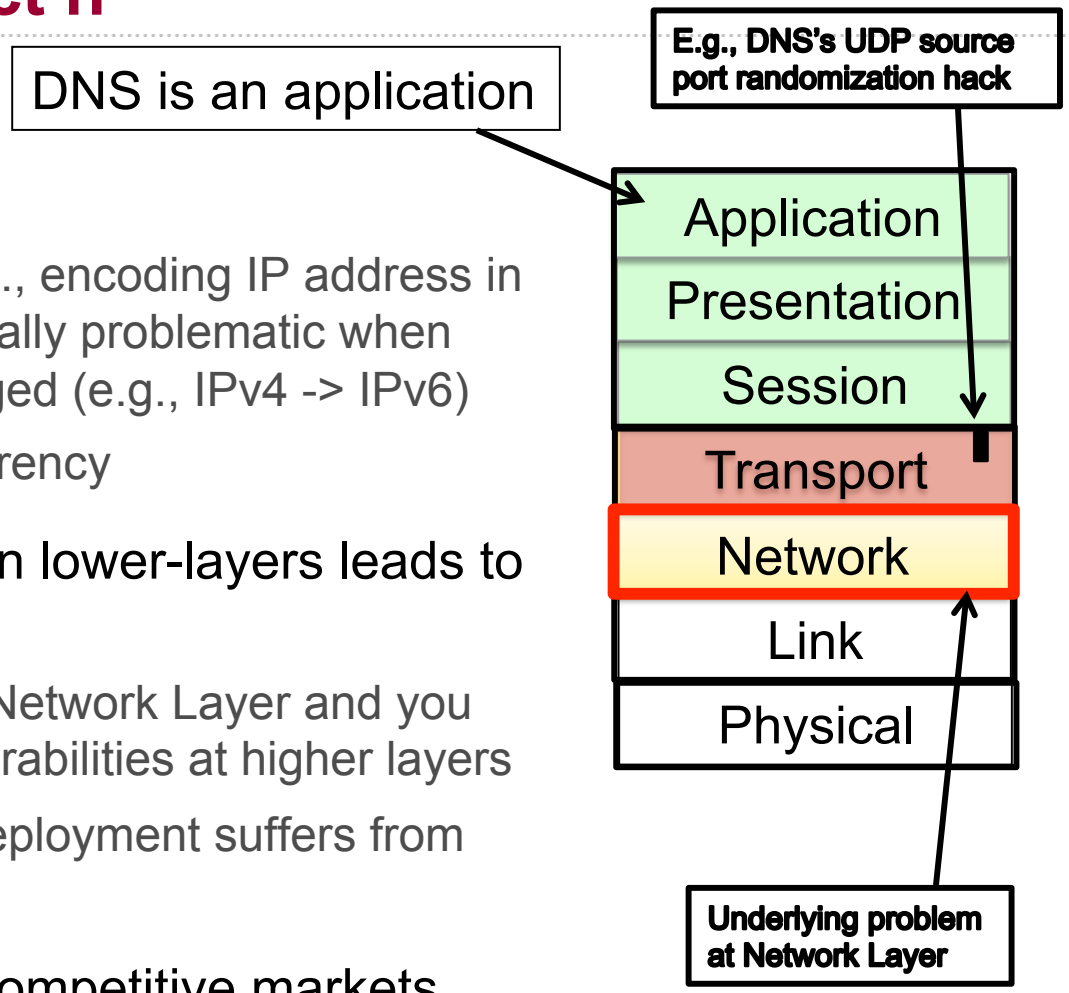
- Ultimate value of DNSSEC deployment can't be realized until recursive name servers and stub resolvers perform validation
  - Some evidence of uptake, but much work still necessary
  - Incentives not aligned between domain owners and who bears cost of validation (ISPs, enterprises) – Comcast/others have announced trials
  - DNSSEC OK (DO) bit set in 50% of queries, ~constant 2+ years!
- Architectural challenges emerging with application-level validation
  - Decoupling system-wide IP host configuration elements (e.g., resolver specifications) via application-specific behaviors problematic
    - Operations, helpdesk and customer support, split DNS, security issues
  - E.g.,Firefox & IE plugins, Google/Chrome Aspirations
  - DNSSEC provides more ways for resolution to fail, enumeration and countermeasures key
- DNSSEC brings integrity and authentication capability to DNS, additional DNS applications already emerging as result

Failures & Vulnerabilities

- Systemic, shared dependencies (no local or 'in country' roots, TLD, or authority servers); most user-desired transactions begin with DNS query resolution set
- DNSSEC provides integrity; challenges response manipulation
  - GARBAGE_IN==GARBAGE_OUT
  - validated_response == truth in input; else { fail! }
  - Availability attack surface expanse (CPU, memory, disk, state && transaction)
- Combinatorial effects: DNSSEC, IPv6, i18n/IDNs, gTLDs

IP Protocol Architect'n

- General principles
  - Avoid circular dependencies
  - Avoid layering violations (e.g., encoding IP address in application content) – especially problematic when referenced lower layer changed (e.g., IPv4 -> IPv6)
  - Preserve end to end transparency
- Assumptions about security in lower-layers leads to vulnerabilities
  - E.g., fix anti-spoofing at the Network Layer and you implicitly fix an array of vulnerabilities at higher layers
  - Source address validation deployment suffers from 'tragedy of the commons'
- In operational systems and competitive markets deployment is driven by incentive
  - Lack of incremental benefit realization and deployability problematic (e.g., v4/v6 dual-stack mess)



The DNS Quandary

truth

DNSSEC
Certificate Carriage
DKIM
Service locator (e.g., MX)
Expanding functions
NAT and NAT-PT (IPv6)
Topologically localized response
Flux (malicious or legitimate)
I18n (and equivalency)
National policies
AAAA whitelisting
Bot containment
Response synthesis
Reputation services
Cache poisoning
Rogue resolvers
Static host records

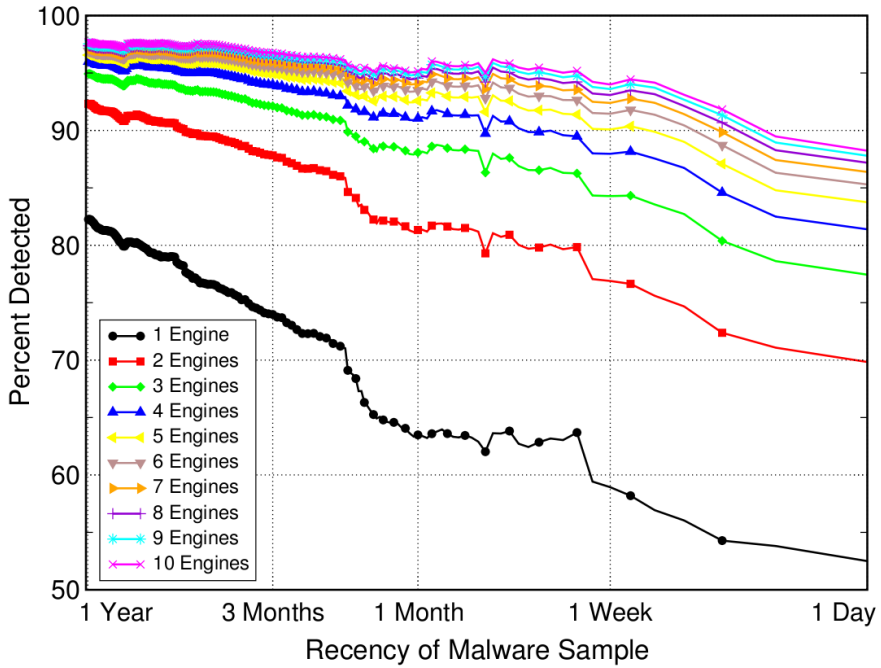
fabrication

The DNS

Inverted Pyramid, Malware Proliferation

- New malcode **every ~11 seconds** in 2009
- 10 AV engines yield only 88% day-1 protection
- Most vulnerabilities ‘client-side’…

Oberheide, et al. N-Version Antivirus in the Network Cloud”, Proc. of the 17th USENIX Security Symposium



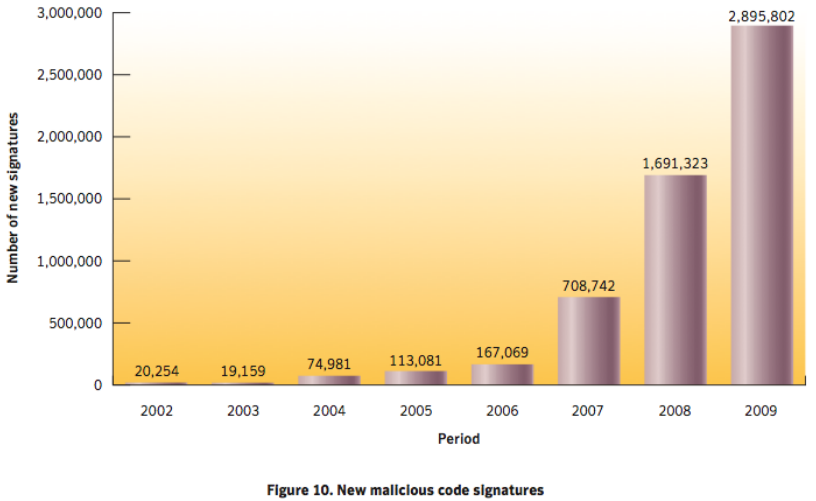
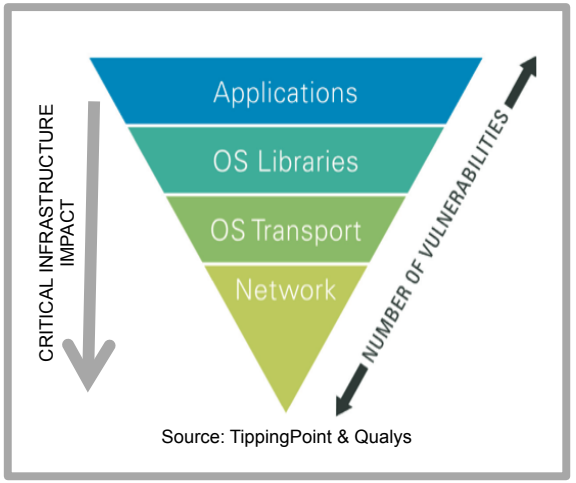


Figure 10. New malicious code signatures
Source: Symantec.

Unique malcode released every 11 seconds in 2009



Source: TippingPoint & Qualys

Malware & Botnet Trends

- Proliferation of compromised end systems and nefarious employment continues
- New domains sometimes used for malice
  - e.g., Conficker variants
- Botnet C&C more sophisticated, resilient to takedown or infiltration
  - IRC, P2P, HTTP, DNS, [Fast] Flux, social networks, twitter, etc..
- Registrant compromise and social engineering increasingly impacting services availability and integrity, in particular with DNS
  - Registrar or managed DNS credentials compromised, zone provisioned redirects to phishing or drive-by download site
- Current protections need augmented (e.g., reputation data)

DDoS Attack Evolution

- Scale – 49 Gbps attacks reported in 2009 Annual Infrastructure Survey; attacks as large as 150 Gbps reported in the media
- Frequency & Duration – Both volumetric and application layer attacks occurring on much more frequent basis
- Sophistication – attacks that exploit middlebox (e.g., load-balancer, firewall, NAT), server, and backend state are becoming more popular, to include attacks with specific exploit vectors…

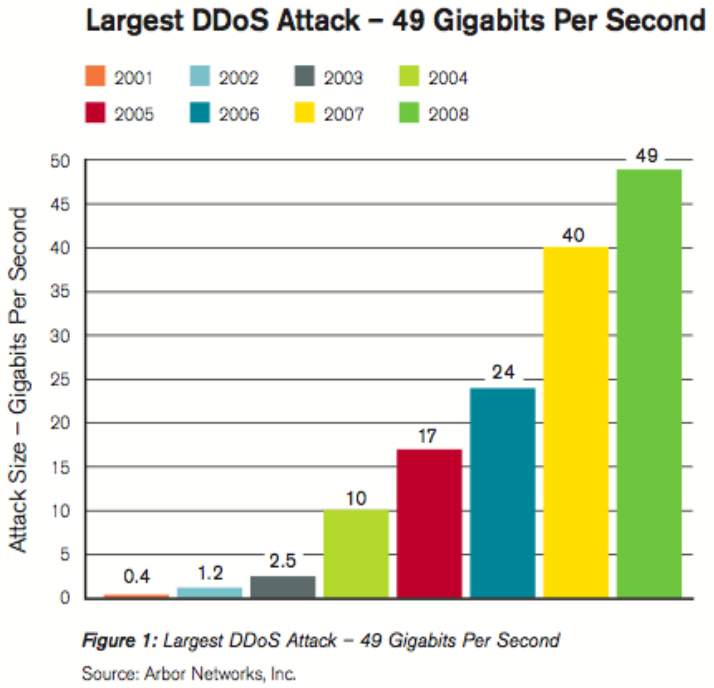


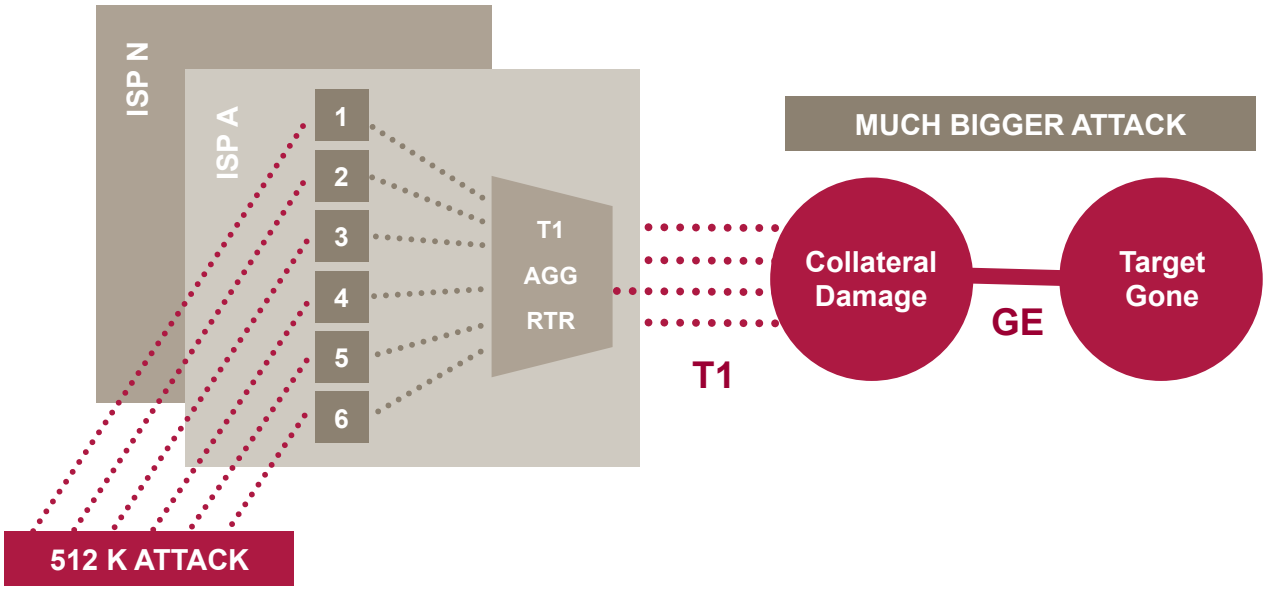
Figure 1: Largest DDoS Attack – 49 Gigabits Per Second

Source: Arbor Networks, Inc.

Fastest discrete IP backbone links today are typically 10 Gbps – large attacks MUST be mitigated "in the cloud"

Collateral Damage

- Botnets take advantage of high-speed access and reflectors for amplification attacks and brute-force flooding attacks
  - 20 Cable hosts w/512K of upstream access can easily generate 1G of attack traffic
- ISPs are taken offline in the process of trying to mitigate these attacks – inband traffic such as routing updates may be dropped due to congestion as well, triggering much wider disruptions



Control traffic contention or sheer traffic volume often results in collateral damage to other customers and network infrastructure.

DNS DDoS Evolution

- Miscreants know that DNS is often easiest impact component for effecting target services – exhibits less capacity than service itself
  - DDoS target commonly authority services
- DNSSEC introduces more overhead across all areas of system, root to stub resolver, expands DoS attack surface considerably
- Growth in tenant densities on authoritative name servers increasingly yielding broader collateral damage
- Niche DNS authority service players often [intuitively] acquire frequent target customers, subsequent attacks impact other zones
- Expressly engineered countermeasures and capacity required
  - Virulence and sophistication of attacks requires application-level and multi-transaction countermeasures
  - Aggregate scale of attacks dictates extensive transaction-servicing capacity (it's not just about the bandwidth)

Compliance != Security

- Information security: confidentiality, integrity & availability
  - Compliance primarily concerned with confidentiality
- Firewalls mandated for transaction-oriented enterprises; break End-to-End
  - First bottleneck when resource exhaustion attacks occur
  - Transport layer encryption nullifies value of payload inspection
  - Miscreant compromise vectors were among earliest adopter of firewall traversal capabilities (e.g., client-side infections)
- Array of sophisticated targeted attack vectors exploit middlebox state capacities
  - AJAX/Web 2.0 attacks with back-end transaction capacity problems
  - Negative caching, search algorithm exploits, dictionary attacks, etc..
- Yet to remain ‘compliant’, >80% of IT security spend goes to firewalls and reactive AV – often ignoring systemic elements
  - Compliance: solving 5-10 year old problems and creating new ones!
- Security _should get you compliance

Cloud Aspirations: The Path to Productivity

- How many elements are in the “productivity path”?
  - Thin client local access loop
  - How many elements from **content to keyboard**?
  - How many additional intermediate network data and control plane elements now exist (e.g., DNS servers, middle boxes, etc..)?
  - How many entities share that infrastructure?
- When utilizing cloud-based services accessibility and availability of those services is evermore critical
  - Traditionally, access loop availability didn’t matter for internal productivity – this changes with *aaS and in-cloud services
  - Collateral damage from attacks, additional insider threats, other new vectors are now introduced
  - Availability of client-cloud datapath more important than ever with applications in the cloud

Fire or DDoS – which is more Probable??

- Most enterprises still connected to Internet at 1 Gbps or slower
- DDoS attack
  - 1 Gbps every 26 minutes
  - 10 Gbps every 3 hours
- Availability of web [service] presence is most important thing to most enterprises
- Several attacks as large as 50 Gbps observed
- Yet few invest in DDoS protection services prior to being hit…

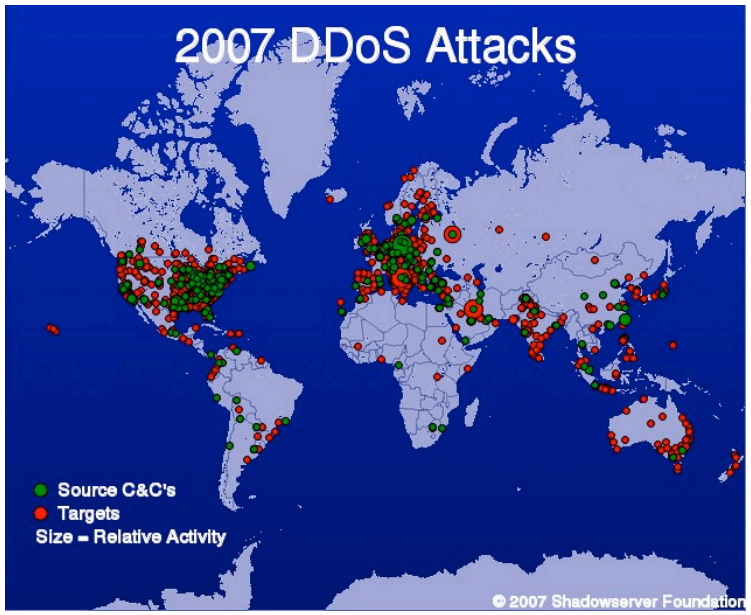
- Fire (North America)
  - Most large enterprises invest > $13.4M* in fire suppression in each DC
  - Yet they have failover between DCs for Internet-facing services
  - The probability of an enterprise having a fire that affects availability of Internet resources is:

    0.000013% Annually* !

*** Numbers in Red were made up, so don't reference them!**

*If you can't touch it or put it in your pocket, people often have a difficult time comprehending it -- **E.g., digital immigrants** that control purse at many critical organizations*

Theoretical ‘Ashlitvia’ Example



- External DDoS driving internal resource exhaustion – need to achieve steady state by blocking ingress traffic from rest of the world
- Nix all international interconnects..
- DNS resolution infrastructure – cached?
- NO Local root servers..
- .ash TLD server no ‘in-country’
- SLD hosted on another continent
- Finally resolves – is user-desired service available ‘in country’?
- Are online certificate status protocol (OCSP) servers reachable? Browser CRL downloads?
- Reverse DNS servers for spam and other AAA-related checks?
- Etc…

On Operating a Global Infrastructure Service

- In order to scale and distribute load at the root and TLD levels, **IP anycasting** is commonly employed
  - Enables IP service address to exist in multiple locations at once
  - Internet operates in ***routing by rumor*** mode – each routing domain makes decisions autonomously (business, customers, peer, routing topology)
  - Scoping anycast route propagation and ***node catchment*** very difficult
- Some governments implement policies influencing various content
  - Modifying DNS responses, including root or TLD
  - IF catchment expands past intended scope, badness happens
  - E.g., MAR 2010 - ‘i root “China exporting censorship” incident

- Route leak detection very complex, response integrity is critical
  - DNSSEC **validation** will address response integrity issue
  - VRSN Innovating new mechanisms for rapid leak detection and enabling preventative policy controls (e.g., per-node discrete origin AS)
  - Developing and adopting foundational elements for secure routing architectures (e.g., RPKI-based resource certification, publication of AS adjacencies)

Sample of DNS Notables…

- .se TLD broken by missing '.'
  - DDoS on specific .se sites following week garnered more attention!
- Checkfree.com – 75% US ACH transactions
  - NS glue redirects enable drive-by downloads; overly automated registrar phishing expedition led miscreants to miss this!
- 'I root' incident with China
  - Anycast catchment expansion results in exportation of national censorship policies
- 'L root' renumbering incident
  - ICANN renumbers their root(L), old IP 'leased' by resource holder – servers on IP respond authoritatively for 6 months
- ICANN, Paypal, Comcast, Facebook, Twitter, ….
  - Registrar or Managed DNS credentials compromise
- DNS Reflective Amplification vector == >50 Gbps attacks
  - 10 residential hosts can easily generate > 1 Gbps attack payload
- Array of DNSSEC related issues already

From Strings to SIGINT >> Reputation

- AV & IDS struggling
  - ~60% avg. protections – necessary but sorely needs to be augmented
- Can learn a lot from behavioral namespace observation
  - root, TLD, authority, recursive, stub, application & registration data
- Augment with statistical/behavioral/relational modeling of telemetry data:
  - Transmission infrastructure (fiber, radio, copper, etc..)
  - Network layer reachability information, AS interconnect topologies, etc..
  - Network transactions (e.g., flow data, misuse, compound temporal)
  - Certificate status checks (e.g., CRL & OCSP)
  - Honeypot darknet instrumentation and website crawling
  - Collect, analyze, categorize malcode (family v. variants, packers & polymorphism)
  - C&C evolution (e.g., IRC, HTTP, DNS, P2P, twitter, Facebook, comments, etc..)
  - Botnet employment (e.g., instruction logging, relational modeling)
  - Data sharing; public and private sector, global, real-time
- Subsequently enact controls: protective, deterrent, reactive

Be Wary Digital Immigrant!

- **Veiled risks** from infrastructure-enabling functions particularly problematic (e.g., DNS, routing, cybercrime)
  - Shared fate & global inter-dependencies; hierarchical non-local transaction and security enabling elements – pretty much everything above the Network Layer
  - Due consideration of multi-national multi-stakeholder Internet ecosystem
  - Individuals have global projection capability

Conclusion

- Internet is at an inflection point
  - focus shifting from transmission to content
  - captive to security attributes of enabling infrastructure
  - New technologies reshaping definition of ‘Internet’
  - IPv4 depletion sure to be a challenging issue in short order
- Governance, convergence, shared dependencies, national security, the global economy; all rely on a working Internet
- Multi-disciplinary approaches with systemic consideration are required in solutions spaces

EOF