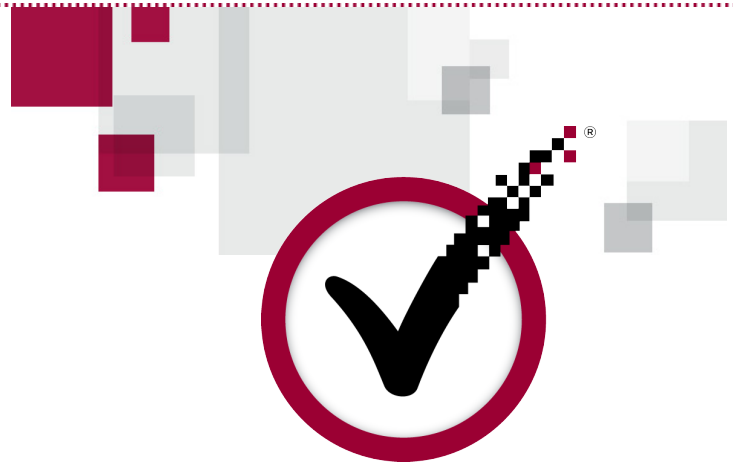
VeriSign®



The Systemic Nature of Internet Threats

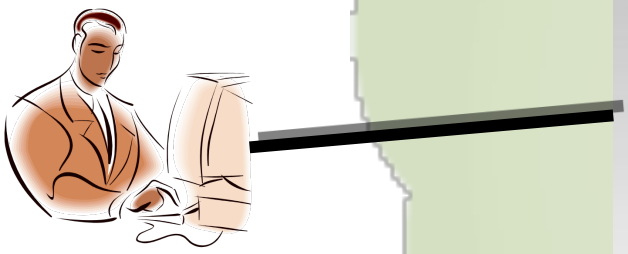
Danny McPherson
Vice President, Research & Development
VeriSign, Inc.

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

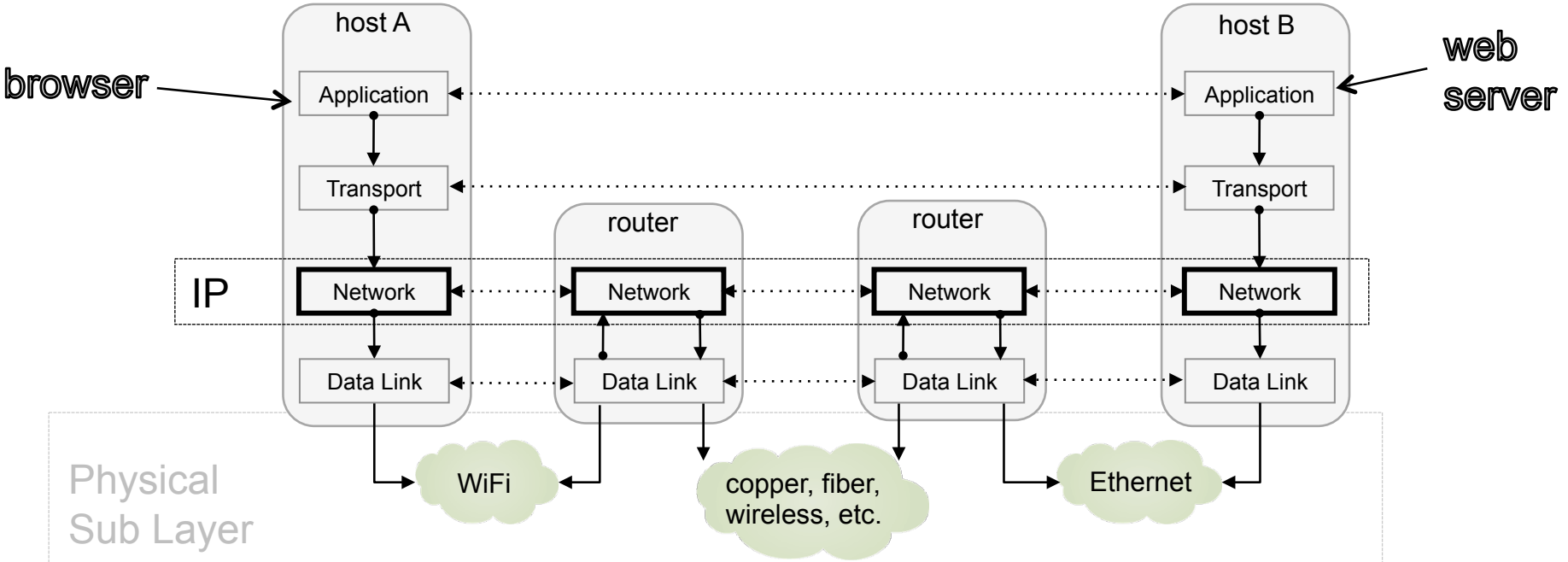
The Internet…



Average user or digital immigrant?

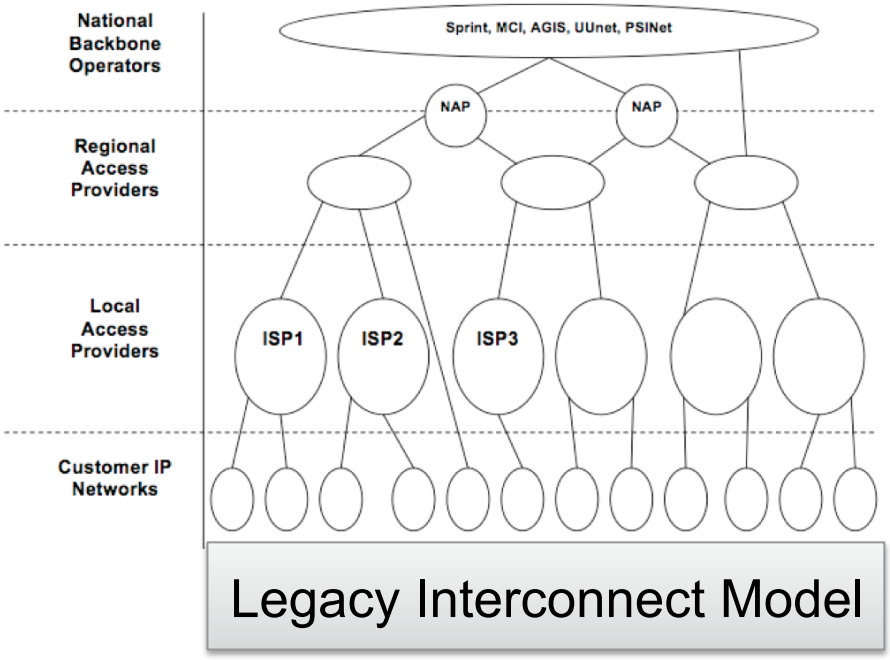
Most users consider the Internet is a big disk drive on the other end of their broadband connection – they don't realize the variables involved in a transaction

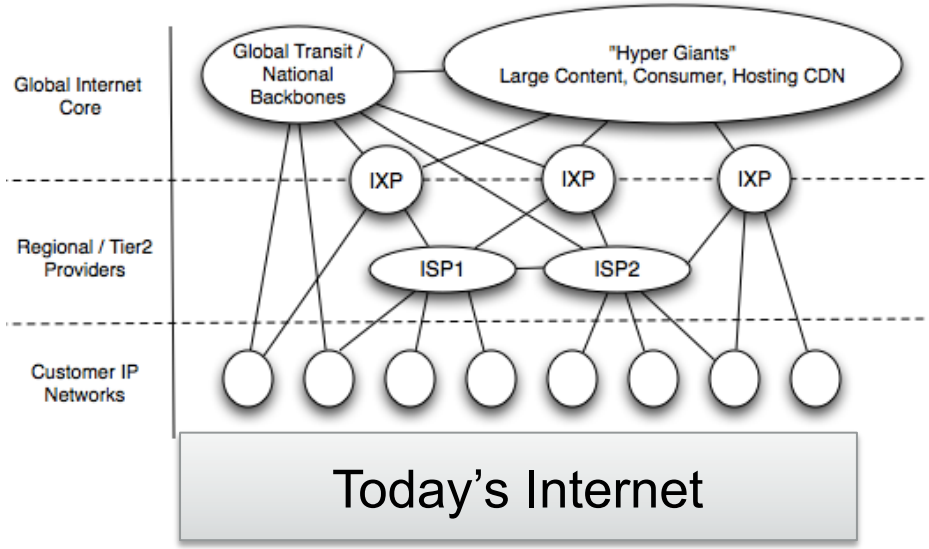
The Internet Protocol Model



- 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

A Flatter Internet; a good thing…

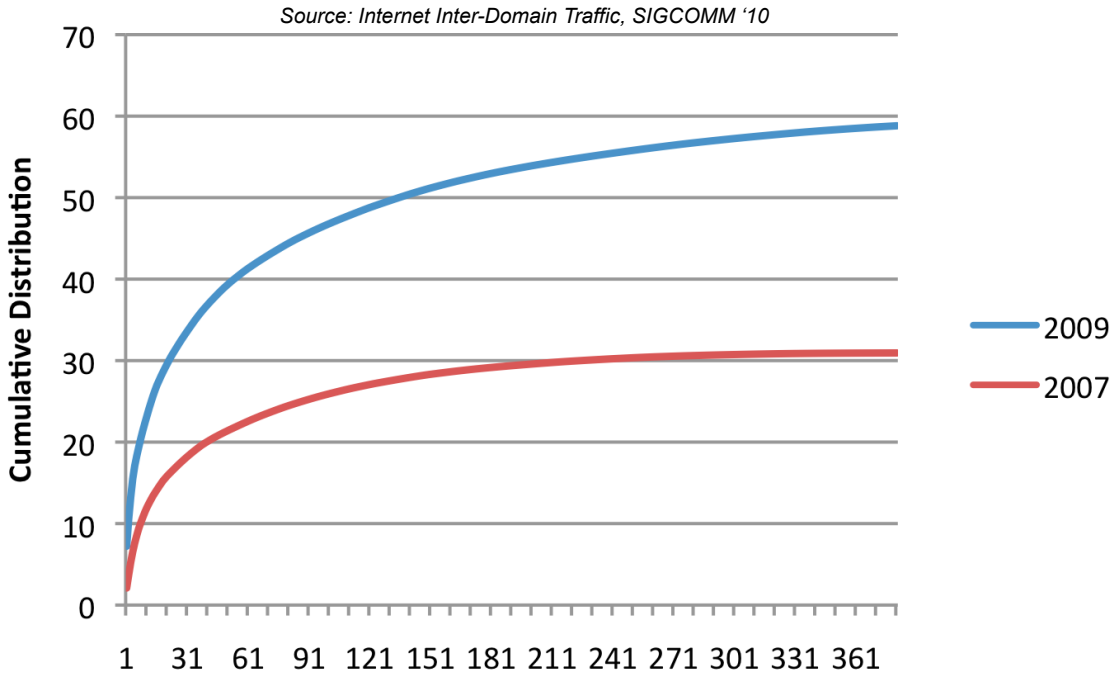




Order of magnitude growth, while mean AS topology 'distance' actually decreased

- 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

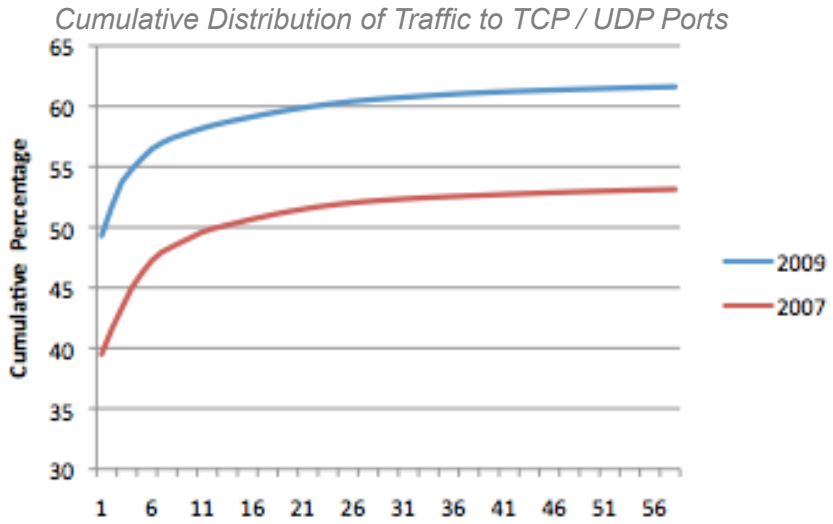


Rank	'09 Top Ten	%
1	*ISP A*	9.41
2	*ISP B*	5.7
3	Google	5.2
4	-	
5	-	
6	Comcast	3.12
7	-	
8	-	
9	-	
10	-	

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 global services, hierarchical systems, and economies of scale; engineering to accommodate is key

However (2) :: And Dwindling End-to-End….

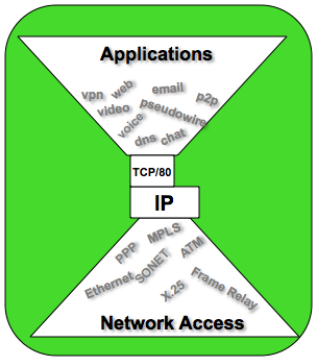


Source: Internet Inter-Domain Traffic, SIGCOMM '10

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?



However (3) :: Transaction Supporting Functions

- IPv4 depletion and IPv6 deployment
  - IPv4 & IPv6 **not** 'bits on the wire' compatible
  - Transitional co-existence expected for decades
  - Risk of fragmenting Internet
- Inter-domain routing on Internet fairly autonomous
  - Flexible, employs "routing by rumor"
  - Internet lacks verifiable number resource authority DB; &security
  - Employment of DB (RPKI) must balance autonomy and security
- Most user-desired transactions begin with name resolution
  - Recursive name server, root, TLD, SLD, reverse DNS – one or more commonly international transactions, even to access local services
  - DNS-based policy fragments Internet
- Certificate status, verification, oft inter-domain multi-national
- Desired or supporting content commonly non-local

However (4) :: DNS Landscape

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

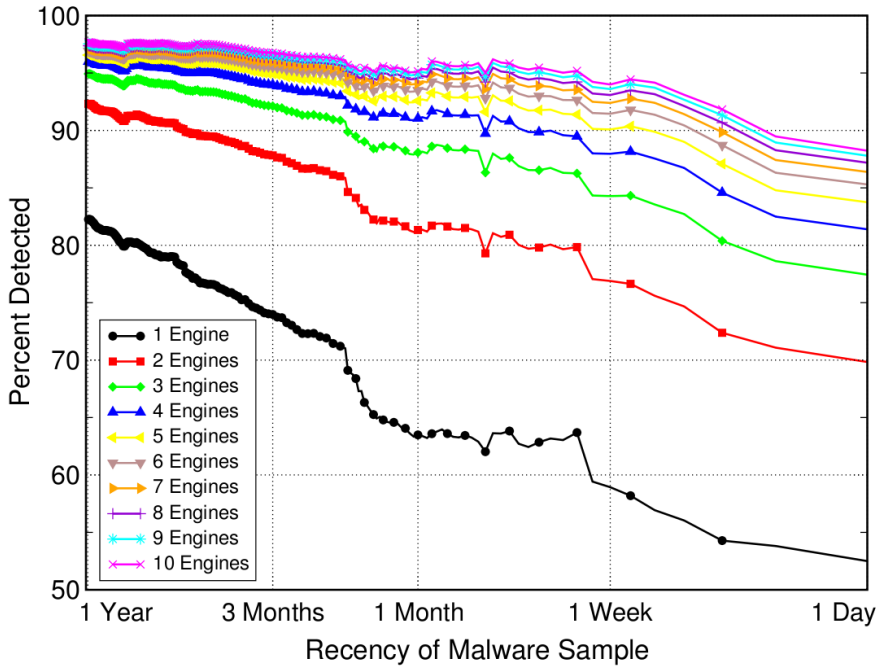
fabrication

The DNS

Even Reactive Controls Insufficient

- 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



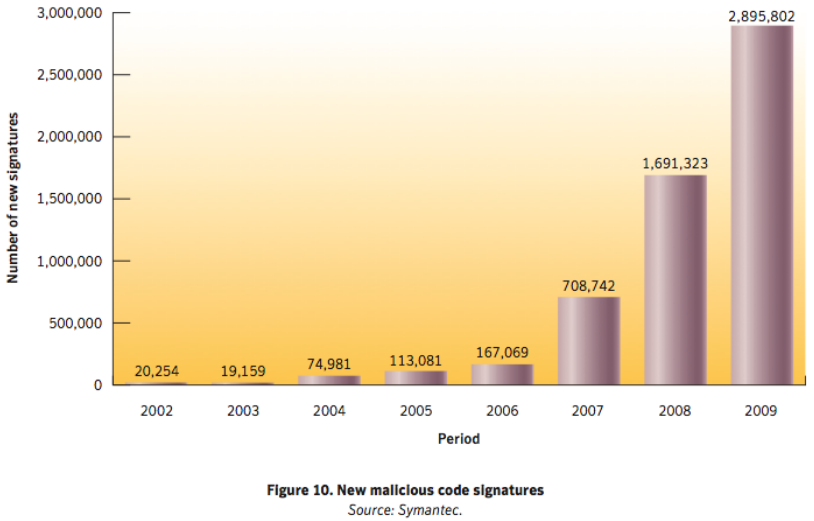
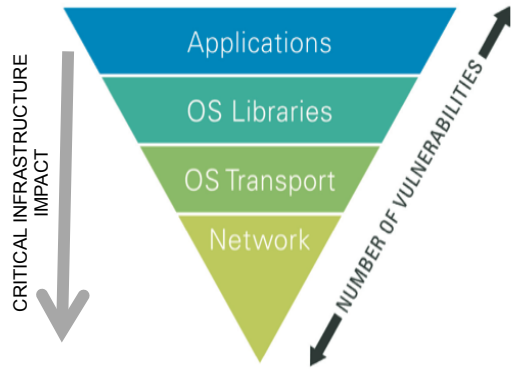


Figure 10. New malicious code signatures
Source: Symantec.

Unique malcode released every 11 seconds in 2009



Source: TippingPoint & Qualys

Be Wary *Digital Immigrant*!

- **Veiled risks** from infrastructure-enabling functions particularly problematic (e.g., DNS, routing, IPv4/IPv6, cybercrime)
  - Shared fate & global inter-dependencies; hierarchical non-local transaction and security enabling elements – pretty much everything above the Network Layer
  - Along with nations, individuals possess global projection capability
- If you can't touch it, or feel it, or put it in your pocket, it's often hard to justify investment or illustrate return; boards, management must embrace

Some Spaghetti..

- If you're not preparing now for IPv6, you're behind
- Must have number resource certification repository, need to balance autonomy needs
- DNS landscape challenging, enables new applications
  - DNSSEC brings integrity, interesting new applications
  - End system, stub resolver split going to be problematic
- Don't build applications that assume authenticity of IP source addresses; lower layers – strive for BCP38 & network ingress filtering deployment
- Compliance doesn't get you security – security SHOULD get you the latter; don't get lazy
  - Firewalls & AV perfect example here…

Conclusion

- Internet is at an inflection point; New technologies reshaping
  - Captive to enabling infrastructure (DNS, IP, routing, etc.)
  - Insurmountable global reliance on working Internet
- Success of Internet driven by any-any end-end; being challenged at multiple levels today
  - Need to avoid islands, partitioning, fragmentation
- Multi-disciplinary approaches with systemic consideration are required in solutions spaces
- Fully enumerated organizational asset valuations must certainly lead to embracing:
  - Internet network & security engineers, multi-national multi-stakeholder policy, data sharing, expanded collaboration
  - Controls to mitigate systemic risks of global Internet ecosystem

EOF