The Myth of Twelve More Bytes
Security on the Post-Scarcity Internet
Technical
- IPv6
- DNSSEC
- gTLDs

Big Picture
- Reputation
- Architecture
- What To Do

Conclusion
- Future Work
Our Conclusions

1. The Internet infrastructure is undergoing fundamental change for the first time in decades
2. The assumption of scarcity is deeply woven into many security assumptions and products
3. The new Internet will face significant problems with trust on both the client and server side
4. New Enterprise Architectures will look very different
5. Everything you have bought will break
The Myth of 12 More Bytes

ARP
Internet Protocol
Link Layer
Physical Layer

Physical Layer
Link Layer
Internet Protocol
DHCP, HTTP, TCP, UDP, ICMP
HTTP, TLS
DHCP

part of nccgroup
The Myth of 12 More Bytes
Come Join the Party
Stateless Address Auto-Configuration

• Give Yourself a local address in your subnet
  • Prefix: fe80:0:0:0:0:
  • IPv6 Address: fe80::f03c:91ff:fe96:d927

• Ask what network you’re in
  • example: 2600:3c03:

• Take your MAC Address, use it in the prefix
  • MAC: f2:3c:91:96:d9:27
  • IPv6 Address: 2600:3c03::f03c:91ff:fe96:d927
Privacy Addresses

• Using your MAC in the last 64 bits identifies you, globally, to every website you visit, no matter where you are
• Super-Mega Evercookie

• RFC 4941 Privacy Addresses
  • Generate a random /64 address
  • Prefer it for outgoing communications
DHCPv6

• Conceptually the same as Original DHCP

• Clients can get more than IP Address
The Default For Windows

- Windows will happily perform SLAAC
- Windows Prefers IPv6 over IPv4
The Default For Windows

• Windows will happily perform SLAAC
• Windows Prefers IPv6 over IPv4

Your computers are just sitting around, waiting for someone to help them talk IPv6

(And it doesn’t have to be you.)
ICMPv6

Critical Infrastructure
SLAAC
Stateless Address Auto-configuration

NDP
Neighbor Discovery (ARP)

MLD
Multicast Listener Discovery

MRD
Multicast Router Discovery

ICMPv6

IPv6
ICMPv6 Protocols

Router Discovery

Who’s a Router?

I’m a Router!
New Protocols
New Protocol Vulnerabilities

(Same Tactics)
Router Discovery

Who’s a Router?

I’m a Router!
Router Discovery

Who’s a Router?

I’m a Router!
Neighbor Discovery

Who’s got 3ffe::1?

That’s me!
NDP Spoofing is the New ARP Spoofing

Who’s got 3ffe::1?

That’s me!
ICMPv6 Protocols

Duplicate Address Detection

Does anyone have 3ffe::45?
ICMPv6 Protocols

Duplicate Address Detection

Does anyone have 3ffe::45?
I do!

Does anyone have 3ffe::46?
I do!
Extension Headers

Pain in the Firewall
### IPv6 Packet Format

<table>
<thead>
<tr>
<th>Version</th>
<th>Traffic Class</th>
<th>Flow Label</th>
</tr>
</thead>
<tbody>
<tr>
<td>Payload Length</td>
<td>Next Header</td>
<td>Hop Limit</td>
</tr>
<tr>
<td>Source Address</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Destination Address</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Fixed Size Header**
### IPv6 Packet Format

<table>
<thead>
<tr>
<th>Version</th>
<th>Traffic Class</th>
<th>Flow Label</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Payload Length</td>
<td>Next Header</td>
<td>Hop Limit</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Source Address</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Destination Address</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Next Header</td>
<td>Extension Length</td>
<td>Options / Padding</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Options / Padding</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Fixed Size Header**

**Extension Header**
Extension Headers + Fragmentation

IPv6 Header
Hop By Hop Header
Routing Header
Fragmentation Header
TCP Header
Data

Fragment 1
Fragment 2
Stateless Filtering is Impossible

IPv6 Header
Hop By Hop Header
Routing Header
Fragmentation Header
TCP Header
Data

Fragment 1
Fragment 2
Translation & Transition Mechanisms

They’re Such Nice Guys.
Translation & Transition

Transition

IPv6 Island
| IPv4 Internet
| IPv6 Island

Translation

IPv6 < -- > IPv4
Transition

6to4
IPv6 Island to IPv4 Network to IPv6 Island
Relies on Nice people to run border routers

6rd or IPv6 Rapid Deployment
6to4 but instead of nice people, it’s an ISP running it, applicable only to their customers

ISATAP
Host supporting IPv6 sits on an IPv4 Network
Can talk to IPv6 Internet, but not the reverse

Teredo
Host supporting IPv6 sits on an IPv4 Network
Magic NAT-punching IPv6 –in-IPv4 to a Teredo Service Provider (Can be open, can be paid)
Allows an IPv6 Server to sit in an IPv4 Network
Translation

NAT-PT

Old, Deprecated
IPv4 or 6 Clients to IPv6 or 4 Servers
Has External IPv4 addresses for Internal IPv6 Servers
Breaks a lot of stuff

NAT64

IPv6 Clients to IPv4 Servers
Fakes a IPv6 Address for the IPv4 Server
I talk to the NAT64 device, it forwards to IPv4
Pairs with DNS64
And More

Time Limits =(}
## IPv6 Enumeration Mechanisms

### Internet-Based

<table>
<thead>
<tr>
<th>Mechanism</th>
<th>Bits</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Address Guessing using OUI</td>
<td>24-26 Bits</td>
</tr>
<tr>
<td>Sequential Address (DHCPv6 or Sysadmin)</td>
<td>8-16 bits</td>
</tr>
<tr>
<td>Reverse Mapping ip6.arpa</td>
<td>Very Efficient</td>
</tr>
</tbody>
</table>

### Limited to Local Network

<table>
<thead>
<tr>
<th>Mechanism</th>
<th>Bits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multicast Echo (^{nmap})</td>
<td>0</td>
</tr>
<tr>
<td>ICMPv6 Parameter Problem (^{nmap})</td>
<td>0</td>
</tr>
<tr>
<td>Multicast Listener Discovery (^{nmap})</td>
<td>0</td>
</tr>
<tr>
<td>SLAAC Fake-out (^{nmap})</td>
<td>0</td>
</tr>
</tbody>
</table>
Yet More

- Multicast!
  - Listener Discovery
  - Listener Enumeration
  - Router Discovery
  - Router Enumeration

- Transition Mechanisms
  - 6to4
  - 6rd
  - 4rd
  - Teredo
  - ISATAP
  - 6in4
  - 6over4

- Node Querying
- UDP/TCP Checksum Calculation

- Router, DHCP, and DNS Discovery
- Redirection
- SeND
- New Features in DHCPv6

- Per-Network Consistent-But-Random Addresses
DNSSEC Chain

att.com
DNSSEC Chain

att.com

ICANN
DNSSEC Chain

Verisign

ICANN

.com

Verisign

att.com
Who verifies the signatures?

Validator

Client
Who verifies the signatures?

Validator → Client
Everything Is Signed

$ dig +dnssec nic.cz +short
217.31.205.50
A 5 2 1800 20120719160302 20120705160302
40844 nic.cz.
IWGHqGORGO0jh4UuZnwx1P2qoCGYDOcHLhJBIQVJm
h6+0Fskr6Sh2dgj
E6BHQJQJ9HuzSDCHOvJkH98QkK4ZUgMCLSN5DHuVc
mJ/J/g5VMjeWS3i
NmLQVmcvpizwfYVo7cuCg1OteazB2QH7JRp+/KhR+Q
+P8tNpDZKe2kEN VMQ=
Everything Is Signed

$ dig +dnssec nic.cz

;; ANSWER SECTION:

nic.cz. 1797 IN A 217.31.205.50

nic.cz. 1797 IN RRSIG A 5 2 1800 20120719160302 20120705160302 40844 nic.cz. Hc3Il+ABELqr2H2jciV80yTg9+ythOo6FkwFkEl0efvRtckrhr8gFfEFCL8 4JY=

;; AUTHORITY SECTION:

nic.cz. 1797 IN NS a.ns.nic.cz.
nic.cz. 1797 IN NS b.ns.nic.cz.
nic.cz. 1797 IN NS d.ns.nic.cz.

nic.cz. 1797 IN RRSIG NS 5 2 1800 20120719160302 20120705160302 40844 nic.cz. aA7A+00QZ0B5G5tVzVZ7bK78YQ0d7W70tQ9Y+q6YyvFkWkFe6N7vTVVwYCRb2dW8ctQ+1wD/9J=

;; ADDITIONAL SECTION:

a.ns.nic.cz. 1797 IN A 194.0.12.1
b.ns.nic.cz. 1797 IN A 194.0.13.1
d.ns.nic.cz. 1797 IN A 193.29.206.1

a.ns.nic.cz. 1797 IN AAAA 2001:678:300::1
b.ns.nic.cz. 1797 IN AAAA 2001:678:10::1
d.ns.nic.cz. 1797 IN AAAA 2001:678:i::1

a.ns.nic.cz. 1797 IN RRSIG A 5 4 1800 20120719160302 20120705160302 40844 nic.cz. Aj/zemlWtY2fW8+XZDPFBXbcOtKSS9ugtq9vQzX/nD7e131/4H3D

b.ns.nic.cz. 1797 IN RRSIG A 5 4 1800 20120719160302 20120705160302 40844 nic.cz. XZBv0rEzg1Rijj1KhjXT/217x7s5EbbRqfe9a2tU3eyOHmudsKPrVM4

c.ns.nic.cz. 1797 IN RRSIG AAAA 5 4 1800 20120719160302 20120705160302 40844 nic.cz. nFX5NMMbodQHYvuw0dOL9qBwRU0sZB+60JGDRsCgGKXIr9VdeAhM

- A/A

b.ns.nic.cz. 1797 IN RRSIG AAAA 5 4 1800 20120719160302 20120705160302 40844 nic.cz. ghUpzvah8F08OvFv23g3/F+dGqQ6🧰TNYoZHBtoyEC6GqT3y757H

c.ns.nic.cz. 1797 IN RRSIG AAAA 5 4 1800 20120719160302 20120705160302 40844 nic.cz. MzB0sPvZqO94fPv2c2g3/F+dGqQ6🧰TNYoZHBtoyEC6GqT3y757H

d.ns.nic.cz. 1797 IN RRSIG AAAA 5 4 1800 20120719160302 20120705160302 40844 nic.cz. MzB0sPvZqO94fPv2c2g3/F+dGqQ6🧰TNYoZHBtoyEC6GqT3y757H
### Signatures Are Large

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Length</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS</td>
<td>77</td>
<td>Standard query A nic.cz</td>
</tr>
<tr>
<td>DNS</td>
<td>259</td>
<td>Standard query response A 217.31.205.50 RRSIG</td>
</tr>
<tr>
<td>DNS</td>
<td>77</td>
<td>Standard query DNSKEY nic.cz</td>
</tr>
<tr>
<td>DNS</td>
<td>1115</td>
<td>Standard query response DNSKEY DNSKEY DNSKEY RRSIG RRSIG</td>
</tr>
</tbody>
</table>

- DNS UDP Limit is 512
- EDNS UDP Limit is 4096
- DNS TCP has no limit

- 24 Residential and SOHO routers were tested
- 18 of 24 Devices tested couldn’t support EDNS
- 23 of 24 Devices tested couldn’t support TCP
Everything Is Signed - Including No’s

Where is doesntexist.att.com?

There is no doesn'texist.att.com
RRSIG(“There is no doesntexist.att.com”, ATT-Key_{ZSK})
Denial of Service

Where is doesntexist1.att.com?
There is no doesntexist1.att.com
RRSIG("There is no doesntexist1.att...", ATT-Key_{ZSK})

Where is doesntexist2.att.com?
There is no doesntexist2.att.com
RRSIG("There is no doesntexist2.att...", ATT-Key_{ZSK})

Where is doesntexist3.att.com?
There is no doesntexist3.att.com
RRSIG("There is no doesntexist3.att...", ATT-Key_{ZSK})
Sign a Single Response?

Where is doesn'texist.att.com?

No Record
RRSIG("No Record", ATT-KeyZSK)
Man in the Middle

att.com

RRSIG("No Record")

att.com

RRSIG("10.6.7.3")
Sign The Ranges

Where is doesn'texist.att.com?

There is nothing between admin.att.com and keyserver.att.com
RRSIG(“There is nothing between...”, ATT-Key_{ZSK})

Called NSEC
Information Disclosure

Where is doesn'texist.att.com?

There is nothing between admin.att.com and keyservers.att.com

RRSIG("There is nothing between...", ATT-Key_zsk)

O RLY?
Hash, then Sign The Ranges

Where is doesnntexist.att.com?

  doesnntexist.att.com -> hash it -> da739562.....
  There is nothing between a847629..... and ff572645.....
  RRSIG("There is nothing between...", ATT-Key\textsubscript{ZSK} )

Called NSEC3!
‘Put It In DNSSEC’
Shoving Stuff in DNSSEC

Example.com?

10.0.1.200
Shoving Stuff in DNSSEC

Example.com?

10.0.1.200
Shoving Stuff in DNSSEC

Example.com?

10.0.1.200

Example.com? What’s your SSL Certificate?

10.0.1.200,

...
Shoving Stuff in DNSSEC

Example.com? What’s your SSL Certificate?

10.0.1.200,

ClientHello

ServerHello, Certificate, ServerHelloDone

...
Shoving Stuff in DNSSEC
Bootstrapping Security
SSL Certs (DANE)
Product Update Checks
SSL Certs (DANE)
Product Update Checks
SSH
  ssh -o "VerifyHostKeyDNS yes"
  RFC 4255
OpenPGP
  gpg --auto-key-locate pka
S/MIME
  draft-hoffman-dane-smime-03
Domain Policy Framework

- Our attempt to unify several DNS security languages into one, extensible meta-language
- Takes advantage of new gTLD program to build special new neighborhood
- Combines a per-gTLD base policy with policy in DNS:

**Base Policy:** $DPFv=1;HTLS=12;DNSSEC=2;STLS=1$

**Received Policy:** $DPFv=2;HTLS=13;STLS=0$

**Resultant Policy:** $DPFv=2;HTLS=13;DNSSEC=2;STLS=1$
New gTLDs

.com  .org  .net
.biz   .museum  .coop
.whatever  .you  .like
Where ICANN Ended Up

ICANN Multi-Stakeholder Model

Board of Directors

President and CEO

ICANN Staff
  MDR - 68
  SV - 11
  DC - 9
  Sydney - 5
  Brussels - 5
  Other US - 11
  Other non-US - 14

ICANN Staff

ASO
  Regional Internet Registries
    AfrNIC
    APNIC
    ARIN
    LACNIC
    RIPE NCC

GNSO
  gTLD Registries
  gTLD Registrars
  IP Interests
  ISPs
  Businesses
  Non-Commercial Interests

ccNSO
  ccTLD registries
    (.us, .uk, .au, .it, .be, .nl, etc.)

At-Large
  Internet Users
    (At-Large Advisory Committee, in conjunction with RALOs)
    ALAC

Security & Stability Advisory Committee
  SSAC

Root Server System Advisory Committee
  RSSAC

Technical Liaison Group
  TLG

Internet Engineering Task Force
  IETF

Governmental Advisory Committee
  GAC

iSECpartners part of nccgroup
Where ICANN Ended Up
Competition and Public Interest
Competition and Public Interest

Most new gTLDs could be closed shops
Kevin Murphy, June 21, 2012, Domain Registries

ICANN’s new generic top-level domain program could create almost 900 closed, single-user namespaces, according to DI PRO’s preliminary analysis.

Surveying all 1,930 new gTLD applications, we’ve found that 912 – about 47% – can be classified as “single registrant” bids, in which the registry would tightly control the second level.

Single-registrant gTLDs are exempt from the Registry Code of Conduct, which obliges registries to offer their strings equally to the full ICANN-accredited registrar channel.

The applications include those for dot-brand strings that match famous trademarks, as well as attempts by applicants such as Amazon and Google to secure generic terms for their own use.

Amazon.com's domain power play: We want to control them all
The e-commerce giant is applying for 76 new top-level domains -- and you won't be able to register any of them. What exactly does it have up its sleeve?
by Paul Sloan | June 21, 2012 4:00 AM PDT
Follow @paulsloan

If Amazon.com gets its way -- and that's still a big if! -- it will soon control 76 new domain extensions on the Internet. Most observers had expected the company to apply for .amazon and .kindle, but it seems that was just for starters: Amazon's ambitions also include a host of generic terms, including the likes of .free, .like, .game, and .shop.

New gTLDs: Competition or Concentration? Innovation or Domination?
by Phil Corwin in Categories: new gTLDs

This guest post was writting by Phil Corwin. Mr. Corwin is Founding Principal of the Virtualaw LLC consultancy and serves as Of Counsel to Greenberg & Lieberman and as for the Internet Commerce Association (ICA), all located in Washington, DC. This post is his personal opinion.

Expect the unexpected. Because it will happen. And it has just happened in the application phase of ICANN's new gTLD program, with potentially profound consequences for the future of e-commerce.

During the three year period between the June 2008 ICANN Board approval of the new gTLD program and its June 2011 vote to proceed to the application stage, and even beyond then in the context of continuing GAC-Board discussions, only one competition issue ever became the subject of heated and protracted debate. And that was whether ICANN’s requirement for registry-registrar separation should be relaxed in concert with the new gTLD program, a question that ICANN eventually answered in the affirmative notwithstanding resistance from some members of the GAC.
Top Level Websites

- Supposed to be outlawed
- How do you represent them
  - http://ai
  - http://ai/
- How does this interact with certificate authorities?
  - We could have bought *.bugatti for less than $10K

Existing A records:
- AC has address 193.223.78.210
- AI has address 209.59.119.34
- BT has address 192.168.42.202
- CM has address 195.24.205.60
- DK has address 193.163.102.24
- GG has address 87.117.196.80
The Big Picture

• The Death of Reputation
• Redesigning Enterprise Networks and Attacks
• External Attacks and Enumeration
• Product Promises and Failures
The End of Scarcity
The Death of Reputation

Scarcity makes certain assumptions reasonably true:

• An individual user has a high attachment rate for a small number of IPs

• A trademarked domain name has likely been taken by the most recognizable holder

• IP spoofing is highly limited in full-connection situations
Uses of IP Reputation

- Anti-Fraud and Adaptive Authentication
  - RSA, SilverTail, EnTrust
- DDoS Prevention and Rate Limiting
  - Arbor Networks, RadWare, every load balancer
- IDS, SIEM and Event Correlation
  - ArcSight, Splunk, Sourcefire

A simple example:

```
rate_filter
  gen_id 135, sig_id 1,
  track by_src,
  count 100, seconds 1,
  new_action drop, timeout 10
```
How can you Adapt?

Switch to “Network Reputation”
- Intelligent detection of subnetting
- Correlation to other data to determine flows
- Positive, not negative reputation
- Con: One bad actor could DoS a popular network
- Con: State table will need to be ginormous, creates another DoS

Filter out network bogons
- Reverse BGP lookups
- Central databases of assigned and utilized spaces

Implement intelligent egress filtering
- Subnet limits no longer good enough, need stateful tracking of assigned IPs
Domain Reputation

• A lot of security thinking goes into securing this relationship:

  www.paypal.com <-> 173.0.84.2

• This is also an important mapping:

  www.paypal.com <-> The Real PayPal with all the Money

• With 1400 potential new gTLDs, this mapping becomes more difficult for consumers to keep in their head

  WhoTF is paypal.rugby?
Domain Reputation Protection

- ICANN nGTLD Rules
  - You need to be heavily engaged right now, coming to ICANN meetings
  - Should be possible to derail .yourbrand via official objection process
- Trademark Clearing House
  - Required part of first 90 days of registration
  - Any trademark works, rules and implementation are in flux
- Sunrise Period
  - Required window for existing gTLD and trademark owners to step to the front of line
  - Easiest and cheapest way to get your gTLD
  - Only lasts 30 days, you’ll need to be ready
- URS
  - Mechanism for suspending (but not taking) second level domains
  - Much more IP-friendly than existing WIPO process
  - Nobody wants to run this for $500/name
A word you will hear often

Homograph!

http://paypal.com

xn--fsquooa.xn–g8w231d

http://paypal.com

xn--fsquooa.xn--g6w251d
PunyCode

http://مثال.اختبار
   xn--mgbhofb.xn--kgbechtv

http://例子.測試
   xn--fsqu00a.xn--g6w251d

http://пример.испытание
   xn--e1afmkfd.xn--8oakhbyknj4f

http://דומם.特斯ט
   xn--fdbk5d8ap9b8a8d.xn--debaoad
Browser Homograph Handling

Internet Explorer
• System language settings
• Does not allow mixed characters

Chrome
• Browser language settings
• Does not allow mixed character sets

Firefox
• Whitelists TLDs, changing

Opera
• Whitelists TLDs

Safari...
Safari Character White List

# Default Web Kit International Domain Name Script White List.

Common
Inherited
Arabic
Armenian
Bopomofo
Canadian_Aboriginal
Devanagari
Deseret
Gujarati
Gurmukhi
Hangul
Han
Hebrew
Hiragana
Katakana_Or_Hiragana
Katakana
Latin
Tamil
Thai
Yi
IPv6 is intended to restore the “end-to-end principal”

Will it?

True IPv6 Enterprises would include:
1. Publicly addressable end-points
2. Firewalls doing actual firewalls
3. NAT64 mechanisms for IPv4 access
4. VPN with sticky addresses, like DirectAccess
Will this happen?

Probably not... more likely:

1. Mix of real IPv6 and NAT
   - Both IP versions running end-to-end for a while, causing lots of access control headaches
   - Large scale NAT64 for native IPv6 clients

2. Lots of public addressing with private routing
   - Using a real prefix doesn’t mean you allow public routing.
   - Controls should include null route tables for specific subnet netmask and firewall rules

3. Proxies will become even more important for egress control
   - Proliferation of network identities makes it important to create artificial checkpoints
   - Proxies can provide authentication and logging not based on IP4/6 address
Pros and Cons for Attackers

Pros:
• Likelihood of routable end-points that can be attacked directly (80’s style)
• ARP Spoofing becomes at least 6 new link local attacks
• Easier to hide attacks, internal compromised machines, control channels
• Multiple IP identities slows down incident response

Cons:
• Finding machines via random IP scanning impossible
• 100% coverage of routable space not possible
• DNSSEC provides some protections if properly deployed
You should submit these talks to BlackHat USA 2013:

• “Denial of Service via IPv6 State Exhaustion”
• “Using and Abusing IPv6 Multicast for Fun and Profit”
• “I Want All the Internets: Hacking with Translation and Transition Mechanisms”
• “This Crap Broke: A Study of Major Vendor Products in an all IPv6/DNSSEC World”
• “IPv6 Covert Channels”
Thank You

Alex Stamos
alex@artemis.net
Artemis Internet

Tom Ritter
tritter@iseccpartners.com
iSEC Partners