Information Centric Networking: DDoS Mitigation and DNSSEC for Namespace Management

Eric Osterweil

With collaborators: Pouyan Fotouhi Tehrani, Jochen Schiller, Thomas C. Schmidt, Matthias Waehlisch, Angelos Stavrou, and Lixia Zhang

1 Weizenbaum Institut / Fraunhofer FOKUS, 2 George Mason University, 3 Freie Universitaet Berlin, 4 Hamburg University of Applied Sciences, 5 UCLA
What is Information Centric Networking (ICN)?

• ICN is a new proposed architectural approach for the Internet
  • Fundamentally enhance the Internet’s scalability and security

• Starting premise: we care about information, *not* where we get it

• Instead of focusing on end-to-end (servers at IP addresses, services, etc.), focuses on *information* (i.e. content)
  • Of course, the security of this approach is recognized as a first-class concern
Why focus on info?

• One reason, content is king!

“...IP video traffic will account for 82 percent of traffic by 2022.”


https://www.sandvine.com/phenomena

Why focus on info? (2)

• Another is growing edge-to-edge Internet services

• More and more, today’s apps don’t need centralized services
  • i.e. Chat, file sharing, even private clouds, etc.

• ICN’s reliance on info has led to names being the architectural bedrock
Names

• Some IP vs. ICN architecture basics...

• In the IP Internet, IP is its “thin waist”

• In ICN (and Named Data Networking, NDN) *names* are the “thin waist”

• IP’s thin waist enabled interoperability of networks

• ICN’s thin waist can enable synergistic interoperability with the IP Internet!

Outline

• ICN introduction

• Using ICN to combat one of the Internet’s most devastating attacks (DDoS)

• Using the Internet’s ecosystem to help bolster an industry ecosystem for ICN (i.e. manage its namespace)
That’s a lot of redundant traffic for the same content!
ICN architecture service model

Traffic is pushed to edge, towards consumers of content

Content is already at edge for edge-to-edge apps, like chat, data sharing, cloud etc...
``To know the road ahead, ask those coming back’’

• ICN architectures have many attractive features, but today’s Internet has proven to be evolutionarily resilient

• In this talk, we will
  • Talk about some tangible/near-term benefits we could see from deploying ICN to help protect us
  • Talk about some important aspects of today’s Internet that ICN would be well-served in adopting
Outline

• ICN introduction

• Using ICN to combat one of the Internet’s most devastating attacks (DDoS)

• Using the Internet’s ecosystem to help bolster an industry ecosystem for ICN (i.e. manage its namespace)
So, [how] can ICN help us today???

• In addition to many other benefits, let’s look at one tangible item... Distribute Denial of Service (DDoS) attacks

• We have endured torrents of roBot Network (``botnet’’) attacks for 20 years, this year [1]
  • Happy birthday, DDoS!

• Using ICN, we now have tools to turn the tide on some of the most devastatingly large attack vectors used for DDoS today!

The DDoS state of the union

• In [1], we detail today’s state-of-the art, for DDoS mitigation

• We are losing ground to attackers

• Larger and larger DDoS attacks are being launched from devices that are increasingly easy for miscreants to acquire

• Our carrier and mitigation network capacities are growing, but, “attacks [are] growing in size faster than network growth.”[2]


To growing tide...

• DDoS attack sizes are growing and growing
• In 2015, DHS announced DDoS Defense (DDoSD program), aimed to one day protect against 1 Tbps attacks
• In 2016, krebsonsecurity.com gets slammed with over 600Gbps attack
• Later in 2016, IoT CCT cameras leveraged to slam OVH with 1.1Tbps attack
• Then in 2016, Dyn gets knocked over by 1.2Tbps attack from Mirai botnet (IoT devices)
Today’s state-of-the-art remediation

- We have mitigation providers (Akamai, Neustar, Cloudflare, etc.)
- Provision enormous capacity networks
- Deploy them across the globe
- Build Deep Packet Inspection (DPI) appliances/machines to ``scrub” traffic
But, the attackers still have advantage

• While providers distribute their footprints, they pay heavily for provisioning and capacity
  • Can’t keep pace with free/readily available/highly distributed attackers (i.e. bots)

• Paying for terabits of global aggregate capacity is way more expensive than free
  • And, DDoS is moving its TTPs from network/transport to application layers

This is an impedance mismatch!
We need a way for our DDoS countermeasures to be as topologically distributed as attackers
ICN reverses the impedance!

• In facing Distributed-DoS, the network should be our greatest countermeasure

• We want DDoS mitigation to occur as close to attack sources as possible
  • Avoid collateral damage (congestion), avoid having to provision mitigation networks, etc.

• This type of behavior is exactly what ICN is good at!

• We want to push remediation out to the edge, just like ICN pushes data!
Using Named Data Networking (NDN)

• NDN is a prime exemplar of an implemented/incrementally deployable ICN architecture

• All data is named in a hierarchical namespace:
  /<provider>/<path>/<data_name>
  /<provider>/<path_2>/<other_data_name>
  /<other_provider>/<path>/<data_name>
  ...

• In NDN, clients acquire content by sending interests to the network, and content authors and caches send data in response

[3] https://named-data.net/
Using NDN to combat DDoS

• Built-in DDoS avoidance: caches

• Don’t allow miscreants to bombard producers

• NDN is DDoS-resistant

• But, miscreants can still bombard with *interests*
Adding FITT to NDN

• Extending NDN’s control traffic and data caching, we have developed *Fine-grained Interest Traffic Throttling (FITT)*[^4]

• When provider detects interest-DDoS, use NDN ctrl traffic (NACK) to squelch at srcs

• Plugs remaining DDoS vector in NDN

• Use the network to push remediation to edges

Lately, IoT devices have hit us the hardest

- Rampant security concerns of IoT device compromise
  - Re: OVH attack ‘16, Mirai attacks ‘16, etc.

- Much focus has circled on how to make IoT devices less vulnerable
  - NISTIR 8228 + NISTIR 8259
  - OWASP
  - etc.

https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project
So, (again) [how] can this help us today??

• NDN and FITT can be deployed *today* alongside/on-top of the IP Internet

• The NDN / FITT network will disable DDoS *attack vector*

• IoT devices provisioned with/behind NDN gateway stack

• Connections to IoT provider/cloud over NDN

• Edge-in, no forklift upgrade, no more DDoS traffic to unsuspecting victims
OK, then why aren’t we there yet?

• NDN (and FITT) present near-term deployable technical solutions

• There turns out to be more to operationalizing Internet infrastructure than *just* technical issues

• ...
Outline

• ICN introduction

• Using ICN to combat one of the Internet’s most devastating attacks (DDoS)

• Using the Internet’s ecosystem to help bolster an industry ecosystem for ICN (i.e. manage its namespace)
Today’s ecosystem with tomorrow’s architecture

• The lynchpin of ICN is its namespace

• But, history has shown that naming (in the Internet) is an extremely complex matter
  • Involves technical details, policy details, monetary considerations, etc.

• The Domain Name System (DNS) has evolved a robust ecosystem

• Here, we propose that today’s Internet has something to offer tomorrow’s ICN, NDNSSEC[5]!

The dichotomy of Internet naming

• Internet naming: namespace → content

• w.r.t. how to manage names:
  ```... the network had better not care...”*```

• Indeed, the mechanisms of NDN are well served by their focus on technical issues

• But, we argue that there is still a demonstrated (separate) need for namespace management

This isn’t DNS, but as the Internet’s 30+ year old de facto its phonebook, what can we learn from DNS’ success?

* ``A Conversation with Van Jacobson,” acmqueue Volume 7, Issue 1, February 23, 2009
Isn’t that what NDN DNS (NDNS)\textsuperscript{[6,7]} does?

Wait...

. . . or even CCN Key Resolution Service (CCN-KRS)\textsuperscript{[8]}?


i.e. has this already been addressed?

Yes

- Regarding many technical aspects
  - SDSI
  - Self-certifying names
  - Trusted Third Parties (TTPs)
  - Etc.

No

- Regarding policy and non-technical aspects
  - Trademarks
  - Legal disputes
  - The operational and industry ecosystem that exists in the Internet today
There will be growing pains...

Technical aspects
• Mapping names to content is critical
• Securing that mapping is a first-order design point
• Scaling all of the mechanisms is critical to producing deployable solutions
• ...
• If industry needed for broad adoption, consider...
  • Has historically brought non-technical considerations

Non-technical
• Names developed commercial value (trademarks, intellectual property, etc.)
• Industry has long since coupled DNS domain names to this
• Technical security gets impacted (i.e. name collisions)
How entries are entered and read from phonebook (IETF for DNS)

How to decide what names should be entered in the phonebook (ICANN for DNS)

But, why did we wind up needing this (for DNS)???

Often contentious
Did DNS really need a non-technical mechanism? Really?

• Well, first it seemed not: technical protocols came from IETF

• Then names became business-critical, and it seemed to need something

• After enough demonstrated need, the DNS community evolved the Internet Corporation for Assigned Names and Numbers (ICANN)

• Is it perfect? No. But, perhaps, “Those who cannot remember the past [may be] condemned to repeat it.”¹

¹ George Santayana, “The Life of Reason: The Phases of Human Progress” Vol. 1, 1905
1994: RFC 1591
“It is up to the requestor to be sure he is not violating anyone else’s Trademark.”

1983: RFC 882
1987: RFC 1034

1985: RFC 882
1987: RFC 1034
1994: RFC 1591

RFC 1296 ← ISC
1996: First court ruling in Germany

Domain names are comparable to “telephone numbers, bank routing numbers or postal codes.”
1997: Court ruling in Germany
Domain names indicate origin and can be related to natural and legal persons.
1983: RFC 882
1987: RFC 1034
1997: Initiating DNS Privatization
1998: ICANN Green/White Paper

1985
1990
1995
2000
2005
2010
2015
2020

RFC 1296 ← ISC
.com boom

Domain names (#)

10^3
10^4
10^5
10^6
10^7
10^8
10^9
10^10
1983: RFC 882
1987: RFC 1034
1997: Initiating DNS Privatization
1998: ICANN Green/White Paper
1999: UDRP Launch
2000: .com boom
2020: dispute cases before WIPO
2003: RFC 3467

"Increasing commercialization of the Internet, and visibility of domain names that are assumed to match names of companies or products, has turned the DNS and DNS names into a trademark battleground."

1983: RFC 882
1987: RFC 1034
1997: Initiating DNS Privatization
1998: ICANN Green/White Paper
1999: UDRP Launch
2006: RFC 4367
“[…] there has been a strong demand to acquire names that have significance to people, through equivalence to registered trademarks, company names, types of services, and so on. There is a danger in this trend […]”
When ICN becomes successful...

- Will we have similar (the same) problems (i.e. will the past be prolog)?
- What can/should we do?

Can we punt?
Can we leverage the solution that exists, w/o changing our technical innovations?

We think, YES we can!

- We think we can synergize the technical design with a separate policy function

Remember, "... the network had better not care..."
Our proposed solution (NDNSSEC)[5]

• Namespace
  “set of names from which all names for a given collection of objects are taken” [3, §8]

• Namespace Management
  a (decentralized) namespace management scheme partitions a namespace into management units, zones [6, §6], which are owned and maintained by an authoritative entity.

Namespace management concept

ICN Namespace $\mathcal{N}$

Zone $\mathcal{Z}_i \in \mathcal{Z}$

Zone owner

Authorizes

Producers

Publish under

Divided into zones
Namespace Management Concept
NDNSSEC

DNS Zone Space

Excerpt of DNS zone records

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Class</th>
<th>TTL</th>
<th>Algorithm</th>
<th>Key Tag</th>
<th>Signature Algorithm</th>
<th>Signature</th>
</tr>
</thead>
<tbody>
<tr>
<td>tools.ietf.org</td>
<td>RRSIG</td>
<td>DNS</td>
<td>1800</td>
<td>A</td>
<td>7</td>
<td>2</td>
<td>1800</td>
</tr>
<tr>
<td>tools.ietf.org</td>
<td>DNSKEY</td>
<td>DNS</td>
<td>1800</td>
<td>A</td>
<td>3</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td>tools.ietf.org</td>
<td>DNSKEY</td>
<td>DNS</td>
<td>1800</td>
<td>A</td>
<td>3</td>
<td>7</td>
<td></td>
</tr>
</tbody>
</table>
Namespace Management Concept
NDNSSEC: DNS Zone Appropriation for NDN

ndnified DNS Zone Space

Excerpt of DNS zone records

```
tools.ietf.org 1800 IN RRSIG DNSKEY 7 2 1800 ...
tools.ietf.org 1800 IN DNSKEY 256 3 6 ...
tools.ietf.org 1800 IN DNSKEY 257 3 7 ...
```
Namespace Management Concept
NDNSSEC: Producer Authorization

ndnified DNS Zone Space

/ /com /org

/org/ietf

/org/ietf/tools

Excerpt of DNS zone records:

- tools.ietf.org 1800 IN RRSIG DNSKEY 7 2 1800 ...
- tools.ietf.org 1800 IN DNSKEY 256 3 6 ...
- tools.ietf.org 1800 IN DNSKEY 257 3 7 ...
- tools.ietf.org 1800 IN DNSKEY XXX X X ...
Namespace Management Concept

NDNSSEC: Producer Authorization

ndnified DNS Zone Space

```
tools.ietf.org 1800 IN RRSIG DNSKEY 7 2 1800 ...
tools.ietf.org 1800 IN DNSKEY 256 3 6 ...
tools.ietf.org 1800 IN DNSKEY 257 3 7 ...
tools.ietf.org 1800 IN DNSKEY XXX XX ...
```
Namespace Management Concept
NDNSSEC: Producer Authorization

ndnified DNS Zone Space

Excerpt of DNS zone records:

```
tools.ietf.org 1800 IN RRSIG DNSKEY 7 2 1800 ...  
tools.ietf.org 1800 IN DNSKEY 256  3 6 ...  
tools.ietf.org 1800 IN DNSKEY 257  3 7 ...  
tools.ietf.org 1800 IN DNSKEY XXX  X X ...  ```
Namespace Management Concept
NDNSSEC: Data Publishing

ndnified DNS Zone Space

Data Packet
/html/rfc882
Meta Info
Content

Producer

Excerpt of DNS zone records

tools.ietf.org 1800 IN RRSIG DNSKEY 7 2 1800 ...
tools.ietf.org 1800 IN DNSKEY 256 3 6 ...
tools.ietf.org 1800 IN DNSKEY 257 3 7 ...
tools.ietf.org 1800 IN DNSKEY XXX X X ...
Namespace Management Concept
NDNSSEC: Data Publishing

ndnified DNS Zone Space

Data Packet
/org/ietf/tools/html/rfc882
Meta Info
Content

prefix w/ zone apex

Producer

Excerpt of DNS zone records
tools.ietf.org 1800 IN RRSIG DNSKEY 7 2 1800 ...
tools.ietf.org 1800 IN DNSKEY 256 3 6 ...
tools.ietf.org 1800 IN DNSKEY 257 3 7 ...
tools.ietf.org 1800 IN DNSKEY XXX X X ...
Namespace Management Concept
NDNSSEC: Data Publishing

ndnified DNS Zone Space

Data Packet

prefix w/ zone apex

Producer

sign

Excerpt of DNS zone records

/tools.ietf.org 1800 IN RRSIG DNSKEY 7 2 1800 ...
/tools.ietf.org 1800 IN DNSKEY 256 3 6 ...
/tools.ietf.org 1800 IN DNSKEY 257 3 7 ...
/tools.ietf.org 1800 IN DNSKEY XXX X X ...
Namespace Management Concept
NDNSSEC: Data Publishing

ndnified DNS Zone Space

Data Packet

prefix w/ zone apex

register

sign

Excerpt of DNS zone records

/tools.ietf.org 1800 IN RRSIG DNSKEY 7 2 1800 ...
/tools.ietf.org 1800 IN DNSKEY 256 3 6 ...
/tools.ietf.org 1800 IN DNSKEY 257 3 7 ...
/tools.ietf.org 1800 IN DNSKEY XXX X X ...
Namespace Management Concept
NDNSSEC: Producer Authentication

ndnified DNS Zone Space

Data Packet
/org/ietf/tools/html/rfc882
- Meta Info
- Content
- Signature

Excerpt of DNS zone records
- tools.ietf.org 1800 IN RRSIG DNSKEY 7 2 1800 ...
- tools.ietf.org 1800 IN DNSKEY 256 3 6 ...
- tools.ietf.org 1800 IN DNSKEY 257 3 7 ...
- tools.ietf.org 1800 IN DNSKEY XXX X X ...
Namespace Management Concept
NDNSSEC: Producer Authentication

ndnified DNS Zone Space

Data Packet

```
/org/ietf/tools/html/rfc882
```

Meta Info

Content

Signature

Excerpt of DNS zone records

```
tools.ietf.org 1800 IN RRSIG DNSKEY 7 2 1800 ...
tools.ietf.org 1800 IN DNSKEY 256 3 6 ...
tools.ietf.org 1800 IN DNSKEY 257 3 7 ...
tools.ietf.org 1800 IN DNSKEY XXX X X ...
```
Namespace Management Concept

NDNSSEC: Producer Authentication

ndnified DNS Zone Space

Data Packet

%organ/ietf/tools/html/rfc882

- Meta Info
- Content
- Signature

retrieves

Consumer

Excerpt of DNS zone records

- tools.ietf.org 1800 IN RRSIG DNSKEY 7 2 1800 ...
- tools.ietf.org 1800 IN DNSKEY 256 3 6 ...
- tools.ietf.org 1800 IN DNSKEY 257 3 7 ...
- tools.ietf.org 1800 IN DNSKEY XXX X X ...
Namespace Management Concept
NDNSSEC: Producer Authentication

ndnified DNS Zone Space

Data Packet
/org/ietf/tools/html/rfc882

Meta Info
Content
Signature

Retrieves
Consumer
Verifies signature

Excerpt of DNS zone records

/tools.ietf.org 1800 IN RRSIG DNSKEY 7 2 1800 ...
/tools.ietf.org 1800 IN DNSKEY 256 3 6 ...
/tools.ietf.org 1800 IN DNSKEY 257 3 7 ...
/tools.ietf.org 1800 IN DNSKEY XXX X X ...
Path forward: evolving form IP to ICN

• We have found that there is a great deal of synergy to capitalize on

• ICN’s architecture has a foundation built on names and their namespace

• Naming in today’s Internet is enabled by a rich ecosystem of evolvable elements

• Today’s elements will unlock the path towards the tomorrow’s Future Internet Architecture
Conclusion and research roadmap

Where we are:
- Identified real-world needs for/from ICN
- Preliminary designs and development
- DDoS prototype and simulations
- Namespace policy mechanism

Where we’re headed:
- Solidify deployment models
- Evaluate performance (synchronization disparities, etc.)
- Evaluate with user studies
- Explore additional use cases
Thank you

Questions?
Bib


Bib (4)


• Named Data Networking (NDN) https://named-data.net/


• Pouyan Fotouhi Tehrani, Luca Keidel, Eric Osterweil, Jochen Schiller, Thomas Schmidt, Matthias Wählisch, NDNSSEC: Namespace Management in NDN with DNSSEC, ACM Conference on Information-Centric Networking, September 2019
Backup
Industry’s role in the Internet’s history

• Commercial incentives have driven considerations in naming
• Successful companies rely on (among other things) name-recognition,
  • Trademarks and naming are important security elements
• DNS is a historical example of successful Internet name management
• Has had a very large component of non-technical innovations and protections
Trust Models

Transitive Trust

a) \( r \rightarrow s \)

b) \( r \rightarrow s \rightarrow s \)

c) \( r \rightarrow s \rightarrow s \)

d) generic entity

direct trust
transitive trust

\( r \) relying party
\( s \) subscriber
\( s \) trust anchor
\( s \) generic entity
# Trust Models

## Certificate Chain Verification Complexity

| Trust Schema | Level 1 (root) | Level i (interim) | Level n (leaf) |  
|--------------|----------------|------------------|---------------|---
| **NDNS**     | \( C_0 \) ← ... \( C_i \) ← ... \( C_n \) \( \geq 1 \) | \( KSK_0 \) ← DKEY \( i \) ← KSK \( i \) ← DSK \( n \) \( \geq 1 \) | \( KSK_n \) ← DKEY \( n \) \( \geq 1 \) |  
| **NDNSSEC**  | DNSKEY \( 0 \) ← NS \( 0 \) ← DS \( 0 \) \( \geq 1 \) | DNSKEY \( i \) ← NS \( i \) ← DNSKEY \( n \) \( = 1 \) |  |  

![Diagram of trust models](image-url)
## Related Work

<table>
<thead>
<tr>
<th>Authentication</th>
<th>$\mathcal{N} \rightarrow \mathcal{T}$</th>
<th>$\mathcal{N} \rightarrow \mathcal{Z}$</th>
<th>Self-auth</th>
<th>Zone Scope</th>
<th>Trust Relation</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNSSEC [10]</td>
<td>✓</td>
<td>✓</td>
<td>✗</td>
<td>$\mathcal{N}$</td>
<td>Decentralized</td>
</tr>
<tr>
<td>Detti et al. [4]</td>
<td>✓</td>
<td>✓</td>
<td>✓*</td>
<td>$\mathcal{I}$</td>
<td>Decentralized</td>
</tr>
<tr>
<td>Venkataramani et al. [11]</td>
<td>✓</td>
<td>✗</td>
<td>✓*</td>
<td>$\emptyset$</td>
<td>N/A</td>
</tr>
<tr>
<td>Farrell et al. [7]</td>
<td>✓</td>
<td>✗</td>
<td>✓</td>
<td>$\emptyset$</td>
<td>N/A</td>
</tr>
<tr>
<td>Wong and Nikander [12]</td>
<td>✓</td>
<td>✓</td>
<td>✗</td>
<td>$\mathcal{I}$</td>
<td>Centralized</td>
</tr>
<tr>
<td>Afanasyev [2, 1]</td>
<td>✓</td>
<td>✓</td>
<td>✗</td>
<td>$\mathcal{N}$</td>
<td>Decentralized</td>
</tr>
<tr>
<td>Mahadevan et al. [9]</td>
<td>✓</td>
<td>✓</td>
<td>✗</td>
<td>$\mathcal{N}$</td>
<td>Decentralized</td>
</tr>
<tr>
<td>DiBenedetto and Papadopoulos [5]</td>
<td>✓</td>
<td>✓</td>
<td>✗</td>
<td>$\mathcal{N}$</td>
<td>Decentralized</td>
</tr>
<tr>
<td>Zhang et al. [13]</td>
<td>✓</td>
<td>✓</td>
<td>✓*</td>
<td>$\mathcal{I}/\mathcal{N}$</td>
<td>Decentralized</td>
</tr>
<tr>
<td>Hamdane et al. [8]</td>
<td>✓</td>
<td>✓</td>
<td>✓*</td>
<td>$\mathcal{I}$</td>
<td>Decentralized</td>
</tr>
</tbody>
</table>

* Denotes self-certification
Conclusions and research roadmap

Where we are:
• Non-technical policy enforcement
• Synergized with ICN
• Deterministic authentication
• No additional infrastructure for certificate revocation

Where we’re headed
• DNS data w/o DNS transport
• Evaluate performance (synchronization disparities, etc.)
• Evaluate with user studies
• Explore feasibility in use cases