Applying the DNS/DNSSEC/DANE Protocol Stack to Digital Emblems

Monday, March 4, 2024
ICANN 79 ccNSO Tech Day

Allison Mankin and Bill Woodcock
Packet Clearing House

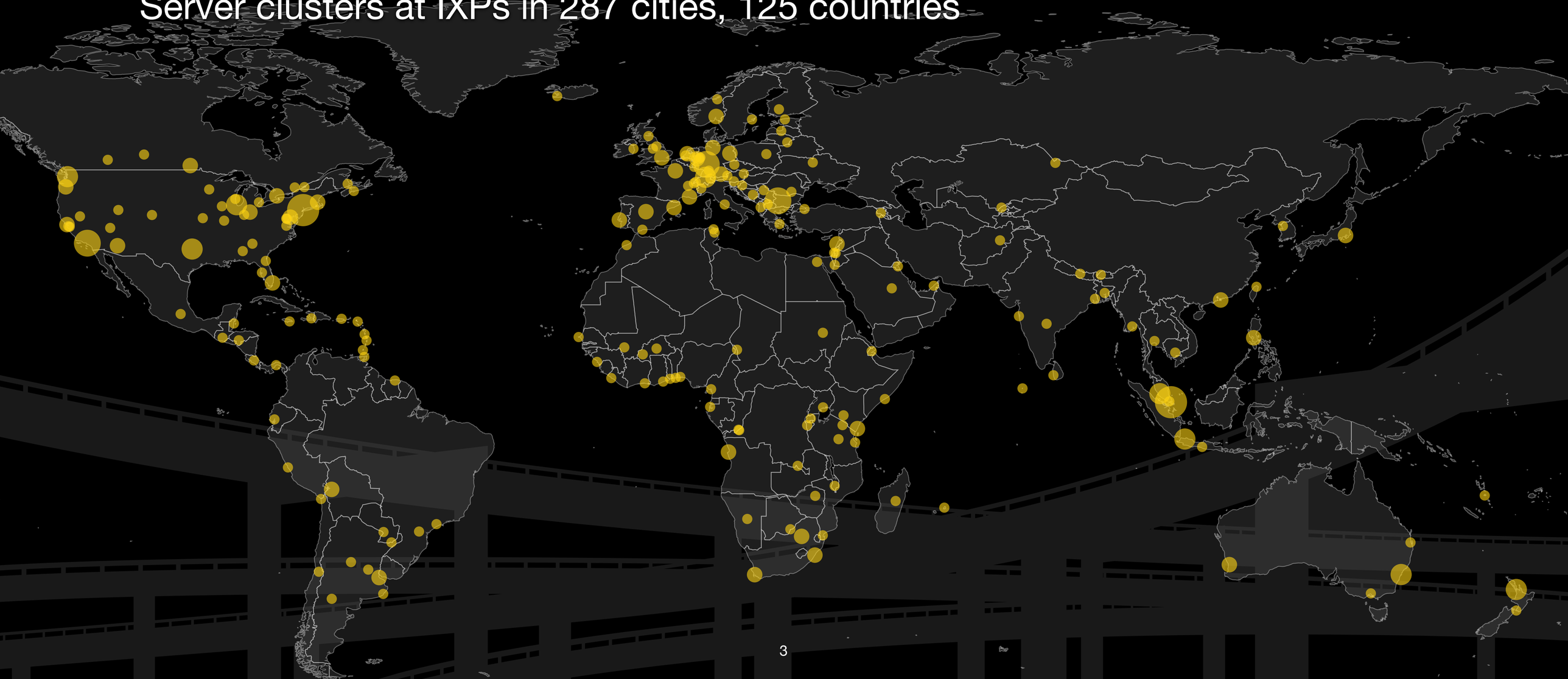
Speaker Intro

Allison has worked in DNS for three decades, author of multiple RFCs on DNS privacy, standards leader for geolocation among other topics at IETF

Her work has spanned DNSSEC and DNS infrastructure, DNS in enterprise, and DNS R&D

PCH works primarily in: the core of the DNS, IXPs, regulatory & policy, and cybersecurity coordination

Server clusters at IXPs in 287 cities, 125 countries



Packet Clearing House

Digital Emblems

Digital Emblems originated because the International Committee of the Red Cross (ICRC) needed cryptographically verifiable version of the protective red cross emblem

The red cross (crescent/crystal) emblem is recognized under international humanitarian law as marking resources which receive protection under the Geneva Conventions

Similar symbols exist to mark cultural heritage, “blue helmet” peacekeeping forces, and “contained dangerous resources” such as nuclear power plants

Packet Clearing House

Digital Emblem Use Cases

A cryptographically verifiable emblem can be used to mark digital assets such as websites, email servers and data-at-rest

It could also be combined with QR codes or RFID to allow verification of the authenticity of physical emblems as well

Initial use case: Digital Emblem (DE) marking the email servers, medical devices and electronic medical systems in a field hospital that is physically marked with the red cross emblem

Packet Clearing House

https://www.icrc.org/en/document/icrc-digital-emblems-report

Packet Clearing House

Digital Emblem Use Cases

Cyber-physical use case example: convoy of trucks some of which have the physical emblem

DE could associate the verifiable emblem with QR-Code on those trucks

DE could associate the verifiable emblem with records for location (of chosen resolution) of the convoy

Packet Clearing House

Digital Emblem and DNS

Cryptographic verification is a combination of digital certificates in DANE with other DNSSEC-signed records

DNS allows association of other records with the entity receiving the emblem, e.g. approver of use of emblem, geolocation (mobile or stationary)

There is IETF work in progress for DNS graphic marker and location records

DNS allows hierarchy for distributed administration, e.g. ICRC and national RCs

Dynamic DNS and DANE allow secure rapid change and revocation

Packet Clearing House

Digital Emblems Effort

PCH is collaborating with ICRC and others (JHUAPL) to develop the resilient, dynamic and secure design for digital emblems

Use existing IETF RFCs including DANE, TXT, LOC and work in progress

Demonstrate in use cases

Prototype simple tool for DE resolution and verification

Work is currently at a milestone: user requirements have been collected and design has been drafted

Novel use of DANE so IETF internet-draft is in preparation

Thanks, and Questions?

https://pch.net

Allison Mankin
Director of DNS Services
Packet Clearing House
allison@pch.net

Additional Background on Packet Clearing House (Not for Presentation)

Packet Clearing House

PCH Intro

Originated as an outcome of the 1992 “National Information Infrastructure” transition of Internet governance from the US government to the global private sector.

Responsible for providing operational security and stability for critical Internet infrastructure globally, much like a “fire department” for the Internet.

PCH works primarily in four areas: the core of the DNS, IXPs, regulatory & policy, and cybersecurity coordination.

Packet Clearing House

A Short History of PCH

Operating production anycast since 1994, precursor organizations since 1989

Advocating for the anycasting of the root nameservers since 1996

Began providing ccTLD nameservice in 1997

Started anycasting root nameservers in 2000

Began providing services over IPv6 in 2001

Anycasted the second DNSSEC-signed ccTLDs in 2006

Started providing FIPS 140-2 L4 DNSSEC key management in 2011

Deployed first DNSSEC-validating, GDPR-compliant, recursive resolver in 2016

Packet Clearing House

PCH and the ccNSO

We currently serve 167 (68%) of you.

For 115 of you, we provide high-performance global anycast DNS.

For 22 of you, we provide FIPS 140-2 Level 4 DNSSEC key management.

For 125 of you, we provide local instances of root, other TLD, and global recursive nameservers.

Packet Clearing House

PCH's Other DNS Services

We currently provide infrastructure for 2 root server administrators:

- D-root (University of Maryland)
- E-root (NASA)
- Infrastructure or assistance for most root server letters over the last thirty years

Global anycast for hundreds of TLDs, by far the largest provider of auth DNS services

- Broadest server footprint, racks of self-owned servers in 287 IXPs in 125 countries
- Only DNS service network large enough to not depend on transit: more than 8,000 peers

Registry services provider

Escrow services with data immunity coming online now

Established and continue to host the Quad9 recursive resolver

- 99.21% effective malware/phishing/stalkerware blocking by independent lab test
- First global recursive resolver to apply DNSSEC validation
- Only global recursive resolver to be GDPR-compliant
- Exempted from law enforcement and intelligence data-collection requirements
- Globally bound by Swiss criminal privacy law

Packet Clearing House

FIPS 140-2 Level 4 DNSSEC key management for 28 countries

Physical security facilities in San Jose, Zurich, and Singapore, with a fourth planned in Montevideo