today's presentation

DNSSEC

By Alan Clegg, ISC.org

the presentation begins at Noon Eastern time

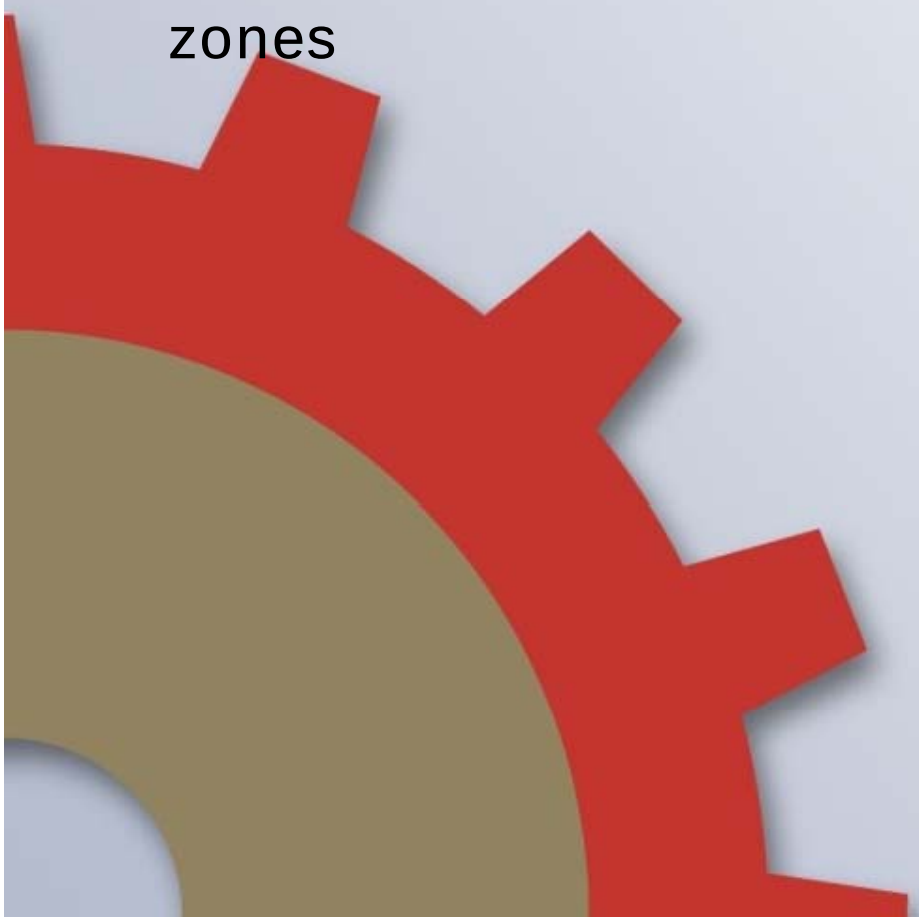
This presentation sponsored by REN-ISAC.

The Research and Education Networking Information Sharing Analysis Center (REN-ISAC) is an integral part of the US higher education strategy to improve network security through information collection, analysis and dissemination, early warning, and response. The REN-ISAC is specifically designed to support the unique environment and needs of higher education and research organizations and efforts to protect national cyberinfrastructure by participating in the formal US ISAC structure.

http://www.ren-isac.net/join

DNSSEC: Loving life after Kaminsky

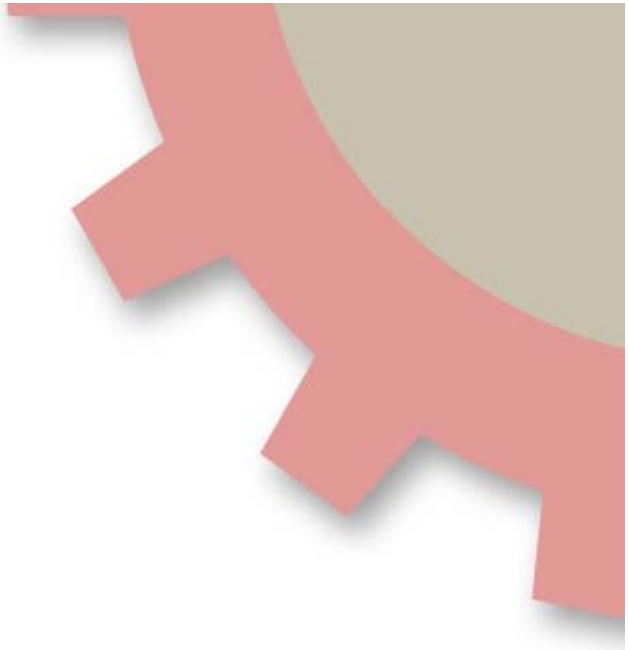
Or: How I overcame my fear and signed my zones



Alan Clegg

Internet Systems Consortium

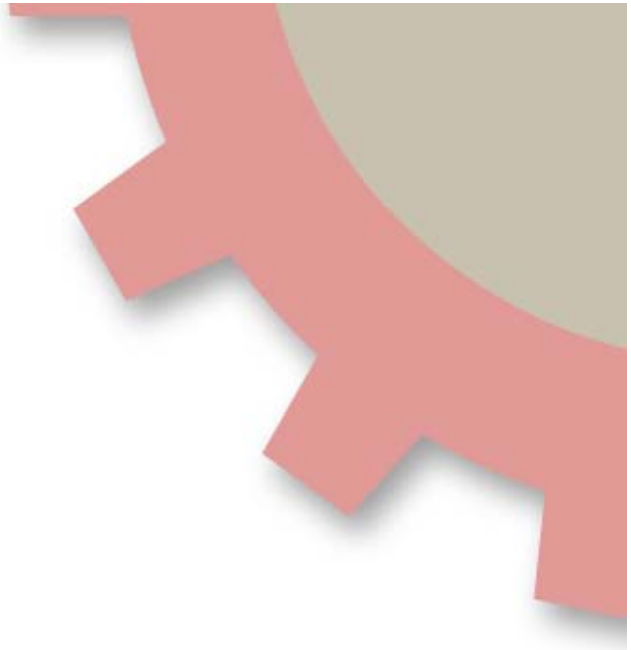
About me...



- Alan Clegg
  - E-Mail: aclegg@isc.org
  - Office: +1-650-423-1357
  - Mobile: +1-919-271-8851

Today's Agenda ...

- 2008, DNS Year in Review
- DNSSEC
  - Introduction
  - Deployment
  - Care and Feeding



2008, DNS Year in Review

2008, DNS Year In Review

- January – Life as normal
- February – Dan Kaminsky makes contact with ISC
- Since then, nothing has been normal...

2008, DNS Year in Review

- In February, ISC, Microsoft, Cisco and other vendors were notified of a new DNS attack vector
- An effort was immediately undertaken to provide software updates that would be released simultaneously across multiple platforms

2008, DNS Year in Review

- On July 8th, 2008, there was a coordinated release by multiple vendors and an accompanying CERT advisory – VU#800113
- The patched code and advisory did not lead to immediate disclosure of the flaw

2008, DNS Year in Review

- On July 21st, an accidental release of additional information occurred
- Dan Kaminsky presented full details of the flaw at the BlackHat conference on August 6, 2008

2008, DNS Year in Review

- On August 28th, 2008, the Office of Management and Budget (OMB) sent out memorandum M-08-23 mandating the deployment and use of DNSSEC for the .gov gTLD

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

August 22, 2008

M-08-23

MEMORANDUM FOR CHIEF INFORMATION

New Policy

This memorandum addresses two important issues in following through with the existing policy and expanding its scope to address all USG information systems.

A. The Federal Government will deploy DNSSEC to the top level .gov domain by January 2009. The top level .gov domain includes the registrar, registry, and DNS server operations. This policy requires that the top level .gov domain will be DNSSEC signed and processes to enable secure delegated sub-domains will be developed. Signing the top level .gov domain is a critical procedure necessary for broad deployment of DNSSEC, increases the utility of DNSSEC, and simplifies lower level deployment by agencies.

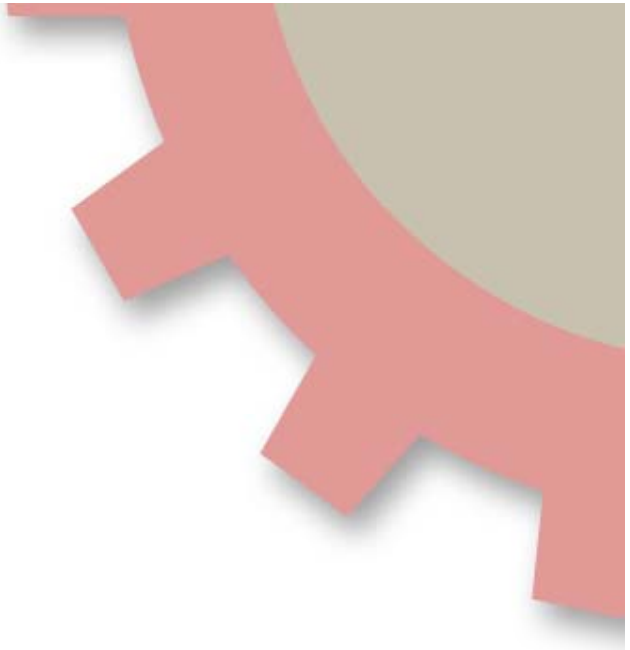
[illegible] use of our networks is important to promote a more citizen centered and results oriented government. The Government's reliance on the Internet to disseminate and provide access to information has increased significantly over the years, as have the risks associated with potential unauthorized use, compromise, and loss of the .gov domain space.

2008, DNS Year in Review

- That brings us to the present
- Wow… what a year!

2008, DNS Year in Review

Questions?

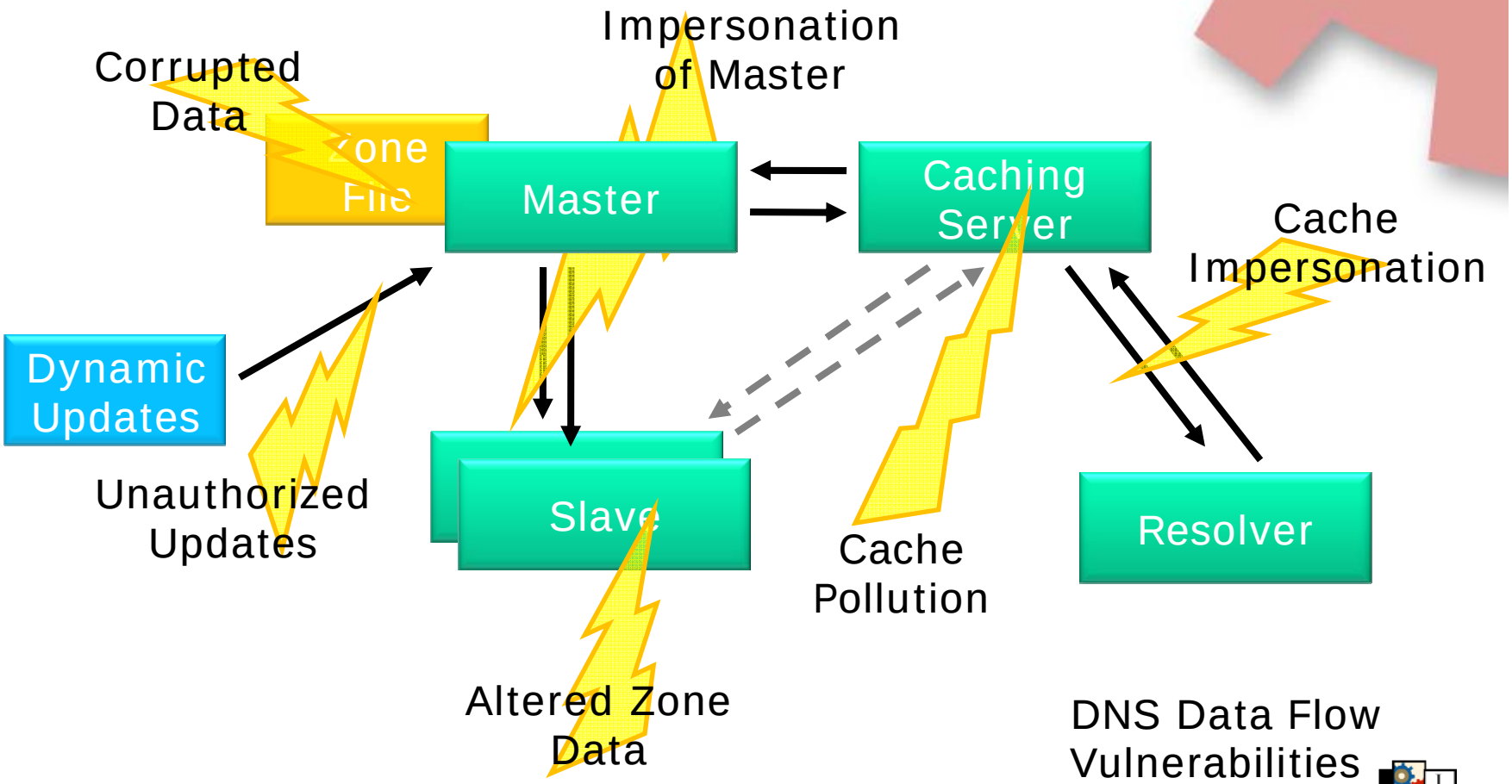


DNSSEC – Introduction

DNSSEC – Introduction

- Contemplate for a moment the amount of trust that we put into the DNS infrastructure
- If DNS were to suddenly become unreliable or untrustworthy, what would the result be?

DNSSEC – Introduction



DNSSEC – Introduction

- DNSSEC provides cryptographic proof that the data received in response to a query is correct
- It does not deal with validating dynamic updates, nor with master to slave data transfers

DNSSEC – Introduction

- Clients using validating resolvers get guaranteed “good” data
  - For some value of “guaranteed”
- Data that does not validate provides a “**SERVFAIL**” response from the upstream resolver

DNSSEC – Introduction

- DNSSEC is based on public key (asymmetrical) cryptography
  - Private key is used to sign DNS data
  - Public key is published via DNS so that validators can retrieve it
  - The public key is then used to validate the signatures, and there-by, the DNS data

DNSSEC – Introduction

- With this knowledge, we are able to prove that data hasn't changed between the authoritative server and the validator, but how do we know we can trust it?
- Once the root (“.”) is signed, that's easy…

DNSSEC – Introduction

- In addition to the “in-zone” signatures and related records, a new entry is required in the parent zone
- A new *Delegation Signer* (DS) record is inserted into the parent, much like the current NS record

DNSSEC – Introduction

- The DS record is a hash of a private key that was used to sign the public portion of the key used to sign the records in the child zone
- By trusting the DS record information, you can trust the information that validates in the child

DNSSEC – Introduction

- BUT WAIT!
- Now we have to trust something in the zone ABOVE the data that we are looking for!
- Remember “Once the root (“.”) is signed, that's easy”?

DNSSEC – Introduction

- DNSSEC is based on chains of trust
- At the top of each chain is a “trust-anchor”
  - One (signed) root, one trust-anchor
  - Until the root is signed, it's not so easy
  - Trust anchors must be gathered and added to DNS configuration

DNSSEC – Introduction

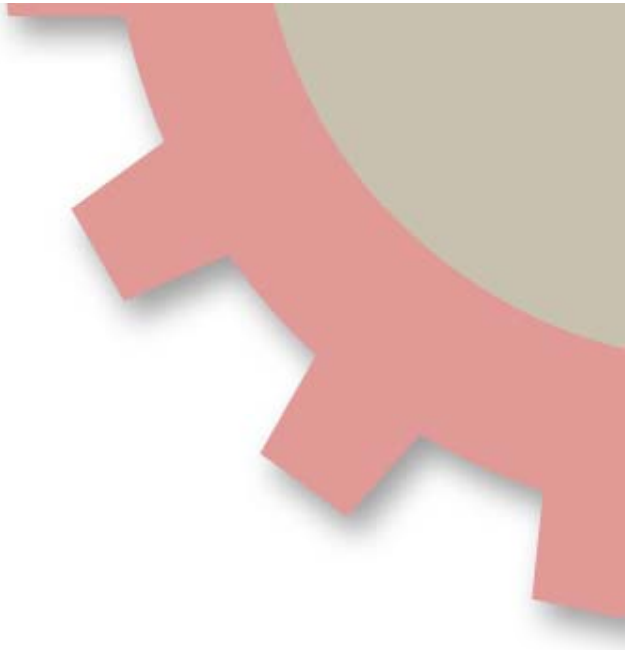
- With the .gov announcement, a single trust-anchor will become available to create the chain of trust for .gov and EVERY ZONE BELOW IT!
- This is very good news

DNSSEC – Introduction

- Recap
  - DNSSEC provides signed DNS data
  - Validating clients can prove that data is “good” or “bad”
  - Chains of trust starting at known trust-anchors must be built and maintained
  - Signed TLDs provide high-level anchors

DNSSEC – Introduction

Questions?



DNSSEC – Deployment

DNSSEC – Deployment

- Recursive servers are the easiest
- Turn on DNSSEC validation
- Add Trust Anchors

DNSSEC – Deployment

```
options {
  dnssec-enable yes;
  dnssec-validation yes;
};
```

- Validation is ONLY done on recursive, not authoritative servers.

DNSSEC – Deployment

- named.conf will need to contain:

```
trusted-keys {
  “gov.” 257 3 5 “BE[...]1ylot7”;
  “isc.org.” 257 3 5 “BEAAAAO[...]ZCqoif”;
};
```

- An entry for EVERY zone apex below which you wish to validate

DNSSEC – Deployment

- Authoritative servers are significantly more difficult

- Turn on DNSSEC
- Create keys to sign DNS data
  - KSK – Used to generate **DS** record
  - ZSK – Used to sign the zone data

DNSSEC – Deployment

- Add KSK and ZSK "**DNSKEY**" records to the zone being signed
- Sign the zone file
  - Creating "**RRSIG**" and "**NSEC**" records
- Modify configuration to use newly signed zone file

DNSSEC – Deployment

<add dnssec-enable to named.conf>

cd /zone/udp53.org

dnssec-keygen -a rsasha1 -b 1024 -n ZONE udp53.org

dnssec-keygen -a rsasha1 -b 4096 -n ZONE -f KSK udp53.org

cat Kudp53*key >> udp53.org

dnssec-signzone -N INCREMENT udp53.org

<change zone file entries to use .signed>

DNSSEC – Deployment

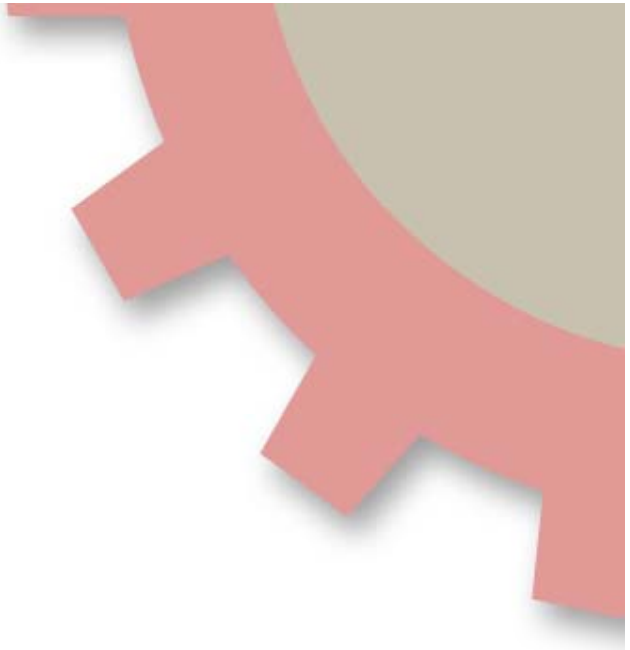
- Having done this and having the nameserver re-read its configuration, you are now serving signed data
- But, you haven't provided your upstream the **DS** records
  - Generated by **dnssec-signzone**

DNSSEC – Deployment

- Recap
  - Enable DNSSEC
  - Create key pairs
  - Sign Zones
  - Provide **DS** records to parent

DNSSEC – Deployment

Questions?



DNSSEC – Care and Feeding

DNSSEC – Care and Feeding

- No good deed goes unpunished
- DNSSEC needs a few special considerations..

DNSSEC – Care and Feeding

- Initially, /zone/udp53.org contained ONLY the zonefile “udp53.org”
- When finished:
  - 2 ZSK files (.key and .private)
  - 2 KSK files (.key and .private)
  - 2 zonefiles (unsigned and .signed)
  - dsset-udp53.org file (DS RRs)
  - keyset-udp53.org file (DNSKEY RRs)

DNSSEC – Care and Feeding

- zonefile began with
  - 71 lines
  - 2,378 characters
- Ended with
  - 665 lines
  - 26,970 characters

DNSSEC – Care and Feeding

- Network and Firewall issues
  - Suddenly, a request for a single address record might return up to 2K of data!
  - If your firewall “fix-ups” DNS records, you might want to make it stop

DNSSEC – Care and Feeding

- Signatures have lifespans
  - “Born-on” date – 1 hour prior to running dnssec-signzone
  - Expiration date – 30 days after running dnssec-signzone
- Expired signatures lead to zones that will not validate!

DNSSEC – Care and Feeding

- Any time you modify a zone – or at least every 30 days (minus TTL) you must re-run dnssec-signzone

- If you don't
  1) Zone data will be stale
  2) Zone will be GONE

     but only to validators!

DNSSEC – Care and Feeding

- Keys need to be rotated
  - No “expiration date”
- The longer a key is in public view, the more likely it is to be compromised
- Compromise (theft) of a key may lead to the need to “roll” a key over

DNSSEC – Care and Feeding

- KSK should be rolled once a year
- ZSK should be rolled every 3 months

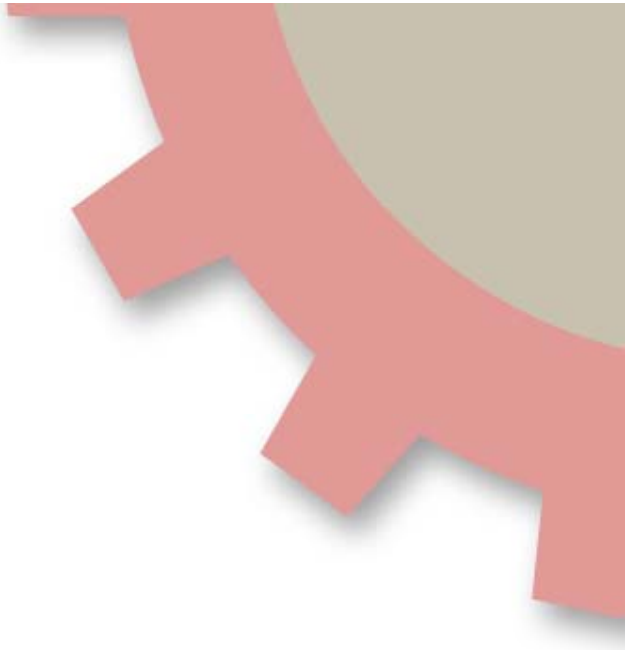
- Procedure is more complex than this presentation will get into

- Automation exists now!

DNSSEC – Care and Feeding

Questions?

About ISC



- Internet Systems Consortium, Inc.
  - Headquartered in Redwood City, CA
  - 501(c)(3) Nonprofit Corporation
- ISC is a public benefit corporation dedicated to supporting the infrastructure of the universal connected self-organizing Internet — and the autonomy of its participants — by developing and maintaining core production quality software, protocols, and operations.