IETF 120 HotRFC
Note Well

This is a reminder of IETF policies in effect on various topics such as patents or code of conduct. It is only meant to point you in the right direction. Exceptions may apply. The IETF's patent policy and the definition of an IETF "contribution" and "participation" are set forth in BCP 79; please read it carefully.

As a reminder:

- By participating in the IETF, you agree to follow IETF processes and policies.
- If you are aware that any IETF contribution is covered by patents or patent applications that are owned or controlled by you or your sponsor, you must disclose that fact, or not participate in the discussion.
- As a participant in or attendee to any IETF activity you acknowledge that written, audio, video, and photographic records of meetings may be made public.
- Personal information that you provide to IETF will be handled in accordance with the IETF Privacy Statement.
- As a participant or attendee, you agree to work respectfully with other participants; please contact the ombudsteam ([https://www.ietf.org/contact/ombudsteam/] if you have questions or concerns about this.

Definitive information is in the documents listed below and other IETF BCPs. For advice, please talk to WG chairs or ADs:

- BCP 9 (Internet Standards Process)
- BCP 25 (Working Group processes)
- BCP 25 (Anti-Harassment Procedures)
- BCP 54 (Code of Conduct)
- BCP 78 (Copyright)
- BCP 79 (Patents, Participation)
- [https://www.ietf.org/privacy-policy/](https://www.ietf.org/privacy-policy/) (Privacy Policy)
IETF meetings, virtual meetings, and mailing lists are intended for professional collaboration and networking, as defined in the IETF Guidelines for Conduct (RFC 7154), the IETF Anti-Harassment Policy, and the IETF Anti-Harassment Procedures (RFC 7776). If you have any concerns about observed behavior, please talk to the Ombudsteam, who are available if you need confidentiality to raise concerns confident about harassment or other conduct in the IETF.

The IETF strives to create and maintain an environment in which people of many different backgrounds and identities are treated with dignity, decency, and respect. Those who participate in the IETF are expected to behave according to professional standards and demonstrate appropriate workplace behavior.

IETF participants must not engage in harassment while at IETF meetings, virtual meetings, social events, or on mailing lists. Harassment is unwelcome hostile or intimidating behavior—in particular, speech or behavior that is aggressive or intimidates.

If you believe you have been harassed, notice that someone else is being harassed, or have any other concerns, you are encouraged to raise your concern in confidence with one of the Ombudspersons.
In-person participants

- Make sure to sign into the session via Datatracker or the QR Code in this session.
- Use Meetecho (usually the “Meetecho lite”) client to:
  - join the mic queue
  - participate in shows of hands
- *Keep audio and video off if not using the onsite version.*

Remote participants

- Make sure your audio and video are off unless you are chairing or presenting during a session.
- Use of a headset is strongly recommended.
The Ground Rules

- **HotRFC is how you make a Request For Conversation**
  - It’s a good way to find IETF people to talk to, for various reasons
- Each person gets four minutes from “Go” to “Please Applaud”
  - At four minutes, we start applauding (see next slide)
  - When you hear applause, please hand the microphone over 😊
- We don’t do questions here - each person provides follow-up info
  - (in-person attendees can follow presenters to the bar, of course)
- So you can follow along, we’re using the datatracker for all slides
  - Let the conversations begin!
Please Applaud!!! (and the crowd goes wild)
IETF 120
HotRFC
What would a post-IETF look like?
PRE-IETF ERA

What did a world pre-IETF looked like?

- Experimental / Proprietary
- Peer to peer / Ad-hoc
- Non-resilient

It made sense to invent commonly agreed Protocols
IETF ERA

What does a IETF world look like?

- Interoperability
- Collaboration
- Agreed optimizations
- Cost reduction

→ The machines still need us
POST-IETF ERA

When the machines don’t need us anymore

- Interoperability > Ad-hoc
- Collaboration > Proprietary
- Agreed optimizations > Ad-hoc
- Cost reduction > Relative

The end of “Protocols”?
QUESTIONS

● The end of “Protocols”?  
● What role could an “evolved IETF” play?  
● How far are we from this scenario?  
● What do we need to prepare so it doesn’t bite us back?
WHAT NOW?

I WANNA HEAR YOUR THOUGHTS ON THIS

- JFQueralt@TheIOFoundation.org
- Side Meeting
  Monday 15:30 - 17:00
  Tennyson room
- Pecha Kucha

(Around all week, anyway)
Thanks!

From Unsplash
CONTACT US

The IO Foundation, a global for-impact NGO advocating for Data-Centric Digital Rights (DCDR)

EMAIL US  SUPPORT US

FOLLOW US

Image credits: Unsplash - Pixabay - Burst
Please Applaud!!! (and the crowd goes wild)
The Multicast Application Ports

Stuart Cheshire
Nate Karstens
Mike McBride

draft-karstens-pim-multicast-application-ports
Working Group: pim
Demultiplexing for Unicast Traffic

• In IP transport protocols, port numbers are used to demultiplex traffic destined to different applications on a host (RFC 7605 §5)
• Traditionally, each application protocol has been assigned a unique port from the IANA registry
• Port assignments are a relatively scarce resource
• When running two copies of the same application on a host static port assignment struggles
• Using a dynamic port and advertising it using DNS-SD has reduced the need for static port assignments
Demultiplexing for Multicast Traffic

• Multicast is more complicated because all hosts in the multicast group must have the same port available
• Hard to coordinate without global static port assignment
• But...
  • Multicast applications *don’t need ports* for demultiplexing!
  • The multicast group destination address *already* identifies the receiving application
• For multicast traffic the destination port field is redundant
  • If a multicast packet arrives at a host, the host should use it!
Multicast Addresses

- Fixed addresses
  - IANA IPv4 & IPv6 Multicast Address Space Registries

- Dynamic addresses
  - RFC 2730 (MADCAP)
  - draft-ietf-pim-ipv6-zeroconf-assignment
  - draft-ietf-pim-gaap
Proposed Solution

• Assign UDP ports specifically for use with multicast applications
  • 49150, 49151 (0xBFFE, 0xBFFF, last two ports of the “user” port range)
  • Consecutive ports to support RTP/RTCP (RFC 3550 §11)

• Conformant applications set SO_REUSEADDR or SO_REUSEPORT
  socket options to share the port with other applications
  • Therefore, host stacks do not need to be updated, though it would be beneficial

• Conformant hosts always act as if these ports are shared
socat Demo

• Transmitter, Terminal 1:
  `socat STDIN UDP4-DATAGRAM:239.0.0.1:49151,ip-multicast-if=172.16.6.100`

• Transmitter, Terminal 2:
  `socat STDIN UDP4-DATAGRAM:239.0.0.2:49151,ip-multicast-if=172.16.6.100`

• Receiver, Terminal 1:
  `socat UDP4-RECVFROM:49151,bind=239.0.0.1,ip-add-membership=239.0.0.1:172.16.1.132,fork STDOUT`

• Receiver, Terminal 2:
  `socat UDP4-RECVFROM:49151,bind=239.0.0.2,ip-add-membership=239.0.0.2:172.16.1.132,fork STDOUT`

Output interface address
Bind to multicast address
Interface address
Receive multiple messages without terminating
How you can help...

• We are interested if there are any application protocols that require more than two ports (consecutive or otherwise) at the same multicast destination address
• Any general feedback is always appreciated
• Attend pim session
  Wednesday Session II (1300-1500) Plaza A
Please Applaud!!! *(and the crowd goes wild)*
Integration of DNS Domain Names into Application Environments: Motivations and Considerations

Swapneel Sheth, Andrew Kaizer, Bryan Newbold, Nick Johnson
ssheth@verisign.com, akaizer@verisign.com,
 bnewbold@blueskyweb.xyz, nick@ens.domains
IETF-120
What are DNS integrations?

• DNS integration:
  • How a DNS domain name is enabled for use as an identifier in an application environment

• Responsible DNS integration:
  • Takes into account qualities and considerations that provide a consistent user experience and extends the security, stability, and resiliency of the global DNS

• Example integrations presented at DINR 2024 Workshop:
  • Bluesky’s social handles
  • ENS’s DNSSEC-based integration
  • Microsoft’s GitHub

• IETF Draft’s goal is to guide applications towards providing responsible DNS integrations
Outline of draft-sheth-dns-integration-00

• Motivations to use DNS domain names in integrations:
  • Global Consistency
  • Stability
  • Flexibility
  • Verifiability
  • Reputation and Brand

• Challenges to consider in DNS domain name integrations:
  • Domain Name Lifecycle
  • Domain Control Validation
  • Completeness
  • Protocol Evolution
  • Identifier Attribution
  • DNS Providers
Next Steps

• Please review the draft and provide feedback
  • Feel free to find us this week
  • Or send us an email during or after IETF

• Working towards adoption by a working group after feedback - is DNSOP the right working group?
Please Applaud!!! *(and the crowd goes wild)*
Stateless Hash-Based Signatures in Merkle Tree Ladder Mode (SLH-DSA-MTL) for DNSSEC

Andrew Fregly
afregly@verisign.com
IETF-120

What is MTL Mode?

MTL Mode is a method for reducing a signature scheme’s operational impact on an expanding message series.

- Rather than signing individual messages, MTL mode signs Merkle Tree Ladders
- Messages are authenticated with Merkle proofs relative to ladders
- Ladders provide backward compatibility since they can potentially verify Merkle proofs constructed relative to future ladders too
- Useful for signature series that sign multiple things at one time. (DNSSEC, OCSP, etc...)
Trade-offs for MTL Mode for DNSSEC

• Benefits
  • Condensed signatures address size issues current NIST PQC signature algorithms present to DNSSEC: A condensed signature in an RRSIG can be comprised of a Merkle proof + reference to signed ladder
    • Limitations related to transmitting large DNSSEC responses over UDP
    • Memory footprint for large zones in authoritative name servers and resolver caches
    • Signing CPU load imposed by some signature schemes (SLH-DSA!)
  • Per our draft for CFRG, “Merkle Tree Ladder (MTL) Mode Signatures” ([https://datatracker.ietf.org/doc/draft-harvey-cfrg-mtl-mode/](https://datatracker.ietf.org/doc/draft-harvey-cfrg-mtl-mode/)), MTL mode operations can be aligned with the underlying signature scheme to ensure proper cryptographic separation
    • Hash-based scheme ➔ quantum-safe design
      • “Stateful” hash-based (if evolving Merkle tree is considered to be state), but graceful degradation of security instead of key compromise if state is reused
    • Hash functions are already available in many hardware platforms, making MTL mode performant
    • Incremental zone signing of RRset batches can significantly reduce CPU requirements. Only one ladder per batch needs to be signed with the underlying signature scheme.
    • Impact of hybrid signatures schemes is minimized as they are applied to signed ladders rather than RRSIGs comprised of condensed signatures
  • Drawbacks
    • Requires a protocol update to support retrieving signed ladders
    • Resolver changes to handle signed ladder caching and full signature production
Overview of draft-fregly-dnsop-slh-dsa-mlt-dnssec-01

• Defines signature formats for both “condensed” signatures and “full” signatures
• Defines the public key format as an SLH-DSA (SPHINCS+) public key.
• Defines the use of EDNS(0) as the means to request full signatures containing signed ladders
• A detailed example containing condensed and full signatures for a signed zone is provided.
Intellectual Property

• Verisign announced a public, royalty-free license to certain intellectual property related to the Internet-Draft

• IPR declarations [6240-6242] give the official language
  (https://datatracker.ietf.org/ipr/search/?submit=draft&id=draft-fregly-dnsop-slh-dsa-mlt-dnssec)
Next Steps

• Please review the draft and provide feedback
• We are looking for partners to participate in interoperability testing
Please Applaud!!! (and the crowd goes wild)
ALFA 2.0 - the Abbreviated Language for Authorization

David Brossard
CTO, Axiomatics

July 21st 2024
I'm Mario
I'm 25
Can I enter Canada to attend IETF?
Authorization Models

Credit: Alex Babeau (3Edges | IDPro): https://idpro.org/a-taxonomy-of-modern-authorization-models/
Standards, Frameworks & Models Timeline

- **XACML** (also SAML) (still not dead)
- **ALFA Profile of XACML**
- **NGAC INCITS 499**
- **UMA v.1**
- **Open Policy Agent (Rego)**
- **JSON Profile of XACML**
- **Zanzibar (Google)**
- **JWT AT OAuth 2.0**
- **OAuth RAR OAuth 2.0**

**Years ago**

- 1992
- 2001
- 2012
- 2013
- 2014
- 2015
- 2016
- 2017
- 2018
- 2019
- 2021
- 2023

**Other Models**

- **ACL**
- **RBAC**
- **ABAC**
HOW STANDARDS PROLIFERATE:
(SEE: A/C CHARGERS, CHARACTER ENCODINGS, INSTANT MESSAGING, ETC)

SITUATION:
THERE ARE 14 COMPETING STANDARDS.

14?! RIDICULOUS!
WE NEED TO DEVELOP
ONE UNIVERSAL STANDARD
THAT COVERS EVERYONE’S
USE CASES. YEAH!

SOON:

SITUATION:
THERE ARE 15 COMPETING
STANDARDS.

Source: xkcd Standards
What is ALFA?

- Abbreviated Language for Authorization
- Implements RBAC, ABAC, ReBAC in one single language
- Drafted under OASIS XACML in March 2014
- Aimed at developers
- All the goodness of XACML, (almost) none of the bad
- Strong uptake within XACML implementations
Who uses ALFA today?

Salesforce uses XACML internally and ALFA to help write policies.

Thales developed the AuthZForce XACML 3.0 PDP as part of Fiware and released via an Open Source initiative called OW2. FIWARE is an open source cloud platform. ALFA is called out in official documentation.

Rock Solid Knowledge have been using ALFA for 5+ years. They have a native C# PDP that uses ALFA which is then “compiled to native”. Their PDP is part of their IAM suite.

Huawei R&D have been using ALFA for 5+ years. They have a native C/C++ PDP that uses ALFA natively to evaluate policies, and a Usage Control (UCON) extension in the form of an ALFA profile that is used as a C/C++ library or via a GoLang service wrapper in various product prototypes including dataspace connectors.

Customers use it to write their policies.
Why ALFA 2.0?

- Get rid of the XACML Baggage
- Strong need for standardized AuthZ
- Promote reuse
- Avoid Cloud platform proprietary options
- Simplify ALFA
Who is interested in ALFA 2.0?

Note: This slide is not an endorsement of ALFA by the parties mentioned.
Next Steps

Questions

• Should ALFA 2.0 be its own WG?
• Should it be part of OAuth? Other WG?

Useful links

• ALFA 2.0 - the Abbreviated Language for Authorization - draft RFC submission
• ALFA reference site: https://alfa.guide
• ALFA Slack Community
Thank you
Please Applaud!!! *(and the crowd goes wild)*
The QuicTLS Project

Rich Salz, Akamai
rsalz@akamai.com
What *was/will-be* QuicTLS?

- **WAS:** A fork maintained by Akamai and Microsoft
  - It *only* added the "de facto QUIC patches"
  - Tracked 1.1 and 3.x pretty closely

- **NOW:** Accept outside contributions; follow the BoringSSL model
  - Pull down (security) fixes from OpenSSL
  - FIPS provider *will still work*
  - Remove "silly things"
  - Address performance
  - Close collaboration with others
Why change?

- The OpenSSL project seems to be all about QUIC
- IETF is about (surprise!) more than just QUIC
We need YOU

- Write/review code/documentation
- Contribute ideas (requirements?)
- Process wonk? Help set up the governance; join the mailing list quictls-setup
- Project: https://github.com/quictls
  Email: https://tinyurl.com/qtls-setup
- Or get in touch with me
Please Applaud!!! *(and the crowd goes wild)*
Privacy.txt: a self-disclosing standard for transparency on the web

HotRFC IETF 120
Privacy on the web

This website uses cookies to ensure you get the best experience on our website. 

Learn more

Got it.

Reading all the privacy policies of the top 20 most visited American websites would take over nine hours. Likewise, reading the privacy policies of the 96 websites a person typically visits in a month would take longer than a full workweek — 46.6 hours. If you spent this time working for a local minimum wage, you would earn approximately $338.14.
ePrivacy Directive and GDPR

- All but necessary data collection requires consent

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Freely-given</td>
<td></td>
</tr>
<tr>
<td>Unambiguous</td>
<td></td>
</tr>
<tr>
<td>Specific</td>
<td></td>
</tr>
<tr>
<td>Informed</td>
<td></td>
</tr>
<tr>
<td>Purpose Limited</td>
<td></td>
</tr>
</tbody>
</table>
Proposed solution: privacy.txt

```
# tudelft.nl/privacy.txt
#
# Entity
Entity: TU Delft
Entity-country: NL
# Privacy policy
Privacy-policy-EN: https://www.tudelft.nl/en/privacy-statement
Privacy-policy-NL: https://www.tudelft.nl/privacy-statement
# Contact
Contact: mailto:privacy-tud@tudelft.nl
Action-delete-personal-data: mailto:fg@tudelft.nl
# Banner
Banner: 1
Consent-platform: non-specific-custom
# Cookies
Cookie: __cookieNotice_consent, .tudelft.nl, 15897600, 0, 0, 0, 0
Cookie: aff_4b3147fdf, www.tudelft.nl, 0, 0, 0, 1, 1
Cookie: fontsLoaded, www.tudelft.nl, 0, 0, 0, 0, 0
```

- Server Side
- Self disclosed
- Machine readable
- Single reference point
Proposed solution: privacy.txt

```
# tudelft.nl/privacy.txt
#
# Entity
Entity: TU Delft
Entity-country: NL
#
# Privacy policy
Privacy-policy-EN: https://www.tudelft.nl/en/privacy-statement
Privacy-policy-NL: https://www.tudelft.nl/privacy-statement
#
# Contact
Contact: mailto:privacy-tud@tudelft.nl
Action-delete-personal-data: mailto:fg@tudelft.nl
#
# Banner
Banner: 1
Consent-platform: non-specific-custom
#
# Cookies
Cookie: __cookieNotice_consent, .tudelft.nl, 15897600, 0, 0, 0, 0
Cookie: aff_4b3147fdf, www.tudelft.nl, 0, 0, 0, 1, 1
Cookie: fontsLoaded, www.tudelft.nl, 0, 0, 0, 0, 0
```
Proposed solution: privacy.txt

```plaintext
# tudelft.nl/privacy.txt
#
# Entity
Entity: TU Delft
Entity-country: NL
# Privacy policy
Privacy-policy-EN: https://www.tudelft.nl/en/privacy-statement
Privacy-policy-NL: https://www.tudelft.nl/privacy-statement
#
# Contact
Contact: mailto:privacy-tud@tudelft.nl
Action-delete-personal-data: mailto:fg@tudelft.nl
# Banner
Banner: 1
Consent-platform: non-specific-custom
# Cookies
Cookie: __cookieNotice_consent, .tudelft.nl, 15897600, 0, 0, 0, 0
Cookie: aff_4b3147f6df, www.tudelft.nl, 0, 0, 0, 1, 1
Cookie: fontsLoaded, www.tudelft.nl, 0, 0, 0, 0, 0
```

Privacy policy information

- [OPTIONAL] privacy policy text
- Privacy policy URL
- + language support
Proposed solution: privacy.txt

Contact information

- General privacy contact email
- [OPTIONAL] Actions:
  - Account and data deletion
  - Personal data deletion
  - Opt out of third-party sharing
  - List of third parties
  - Opt out of marketing
Proposed solution: privacy.txt

```plaintext
# tudelft.nl/privacy.txt
#
# Entity
Entity: TU Delft
Entity-country: NL
# Privacy policy
Privacy-policy-EN: https://www.tudelft.nl/en/privacy-statement
Privacy-policy-NL: https://www.tudelft.nl/privacy-statement
# Contact
Contact: mailto:privacy-tud@tudelft.nl
Action-delete-personal-data: mailto:fg@tudelft.nl

# Banner
Banner: 1
Consent-platform: non-specific-custom
# Cookies
Cookie: __cookieNotice_consent, .tudelft.nl, 15897600, 0, 0, 0, 0
Cookie: aff_4b3147fd, www.tudelft.nl, 0, 0, 0, 1, 1
Cookie: fontsLoaded, www.tudelft.nl, 0, 0, 0, 0, 0
```

Banner information

- [OPTIONAL] banner present
- [OPTIONAL] consent platform
Proposed solution: privacy.txt

```plaintext
# tuudelft.nl/privacy.txt
#
# Entity
Entity: TU Delft
Entity-country: NL
# Privacy policy
Privacy-policy-EN: https://www.tudelft.nl/en/privacy-statement
Privacy-policy-NL: https://www.tudelft.nl/privacy-statement
# Contact
Contact: mailto:privacy-tud@tudelft.nl
Action-delete-personal-data: mailto:fg@tudelft.nl
# Banner
Banner: 1
Consent-platform: non-specific-custom
# Cookies
Cookie: __cookieNotice_consent, .tudelft.nl, 15897600, 0, 0, 0, 0
Cookie: aff_4b3147f1df, www.tudelft.nl, 0, 0, 0, 1, 1
Cookie: fontsLoaded, www.tudelft.nl, 0, 0, 0, 0, 0
```

Cookie information

- For each cookie:
  - Name
  - Domain
  - Duration
  - First / third party
  - Optional
  - HTTP-only
  - Secure
Advantages of privacy.txt

- Machine Readable
- Easy to adopt
- No change on user side
- Does not interfere with browser functionality
- Complete in most important parts of GDPR compliance
- Potential for high accountability
- Transparency as priority
Supporting Tools

Data collector tool 1

- Creation of privacy.txt files
- Verification of privacy.txt files
- Auditing

Cookie compare tool 2
01. Empower users
   - By providing privacy transparency

02. Help websites comply
   - By ease of verification of privacy features

03. Facilitate auditing
   - With large-scale auditing tools
To sum up

01. GDPR compliance on the web is low
02. Privacy.txt as transparency solutions
03. Auditing and Generation Tools

We are looking for collaborators and reviewers feedback on the document or a path forward
References

Please Applaud!!! (and the crowd goes wild)
Online TLS Secure Element for Low-Power High-Security Personal Servers

Pascal.Urien@Telecom-Paris.fr
Pascal.Urien@EtherTrust.com
Motivation

- On-line vault for internet users (individuals, small & medium size businesses)
  - On-line secure elements
  - 10 billions secure elements are manufactured every year, among which 6 billions of javacards, which are programmed with a subset of the java language (i.e. javacard)
  - High security level: EAL6+ (according to Common Criteria standards)
- Open technologies
  - No Non-disclosure Agreements (NDA)
  - Open hardware, for example Arduino Integrated Development Environment (IDE)
- Services
  - Key Management System (KMS)
  - Secure Storage
**TLS-SE**

- TLS for Secure Element (TLS-SE [1])
  - a TLS1.3 pre-shared-key (PSK) profile for secure elements (SE)
- 2 kinds of servers
  - Nano servers, are working with a single element
  - Personal servers are using grids of secure elements
- Uniform Resource Identifiers (URI) for Secure Element resources
  - schemeS://sen:psk@server.com:port/?query

IETF 120 - HotRFC
Personal Server

schemeS://sen:psk@server.com:port/?query

TCP/IP HOST

Secure Element Processor (SEP)

Grid of Secure Elements

On-Demand TLS-SE-APP use the RACS (Remote APDU Call Secure [4]) protocol (ISO7816/TLS-PKI)

IoSEv5 Server (Internet of Secure Elements [3] [6])

Raspberry Pi, Ubuntu, Windows

- SEP= Arduino IDE+ ISO7816 LIB
- Oracle Javacard SDK

IETF 120 - HotRFC
Nano Server

```
schemeS://sen:psk@server.com:port/?query
```

TCP/IP HOST  Secure Element

NET-WORK

ISO7816 Interface, Other

- Arduino IDE
- Oracle Javacard JDK
Low Power Consumption

<table>
<thead>
<tr>
<th></th>
<th>Personal Server</th>
<th>Nano Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>HOST</td>
<td>HOST</td>
<td>HOST</td>
</tr>
<tr>
<td>RASPi 3B</td>
<td>ESP32+Wi-Fi</td>
<td></td>
</tr>
<tr>
<td>SEP</td>
<td>0,10W</td>
<td>0,2W</td>
</tr>
<tr>
<td>SE</td>
<td>0,05W</td>
<td>0,05W</td>
</tr>
</tbody>
</table>

| Power Consumption     | 1,60 W          | 0,2W        |

- Nano Servers [5] may be powered by solar panel
- TLS-SE-IO ([2] a kind of Remote Call Procedure, RCP) can be used to monitor battery charging

\[ V_{R3} = I_{BAT} \times R_3 / 1200 \]

\[ I_{BAT} = \frac{0.2W \times 3.3V}{60mA} \]

\[ V_{R3} = \frac{0.2W \times 3.3V}{60mA} \]

\[ I_{BAT} = \frac{0.2W \times 3.3V}{60mA} \]

\[ V_{R3} = \frac{0.2W \times 3.3V}{60mA} \]

\[ I_{BAT} = \frac{0.2W \times 3.3V}{60mA} \]

\[ V_{R3} = \frac{0.2W \times 3.3V}{60mA} \]

\[ I_{BAT} = \frac{0.2W \times 3.3V}{60mA} \]
Looking for:

- We are looking for partners to develop applications for internet users enabling use of open trusted services.
- Concise Binary Object Representation (CBOR) for shell commands over TLS
- More details:
Please Applaud!!! *(and the crowd goes wild)*
High-performance WAN

Daniel Huang/Quan Xiong(ZTE)

IETF 120 HotRFC, July 2024
Use Cases and Motivation

- Aims to discuss the scenarios and use cases that certain services require effective high-throughput massive data transmission in WANs which called **High-performance WANs (HP-WAN)**.
- Problems may be considered for long-distance connection and massive elephant flows data transmission.

**Scenario A: Single Site** (e.g. <10km)
- **HPC**
- **AI Training**

**Scenario B: Multiple Sites**
- **B.1 Long-distance Transmission between two Sites** (e.g. >1000km):
  - **HPC for Scientific Research**
  - **Distributed Storage**
  - **Data Express Service**
  - **Multimedia Content Production**
  - **Data backup and Disaster Recovery**
- **B.2 Multiple DCs Interconnection** (e.g. >100km):
  - **Collaborative Training across Multiple DCs**

High-performance WANs (HP-WAN)
Objectives and Requirements

• What are the characteristics for HP-WAN?
  • Massive elephant flows data with large burst, concurrent services co-existed with dynamic flows (e.g. 10G~400Gbit/s)
  • Long distances, multiple hops, paths and domains between DCs or from a site to DC (e.g. >100km, >1000km)

• What are the objectives and goals for HP-WAN?
  • The primary goal is to achieve effective high-throughput transmission which demands higher network performance
    • ultra-high bandwidth utilization
    • ultra-low packet loss ratio
    • low latency and jitter

• What are the gaps for existing technologies?
  • Optic Fiber direct connection (e.g. OTN)
    • limited scale and deployment and high cost, requires using IP network resources
  • DC Technologies (e.g. PFC)
    • slow feedback and high Round-Trip Time (RTT) latency and jitter, requires improving flow control precision
  • L3 Routing Technologies (e.g. ECN/ECMP)
    • network is passive and unaware of the status, requires coordination with the end systems
    • network resources is insufficient with low utilization rate, requires improving bandwidth utilization
    • long-distance transmission requires ultra-low packet loss, latency and jitter guarantees
IETF120 Side meeting for High-performance WAN

• HP-WAN Side Meeting Planning
  • Start a discussion about use cases, problems, motivations and requirements of High-Performance Wide Area Networks to achieve high-throughput transmission.
  • **Time:** Tuesday 23 July-15: 30~17:30 (Vancouver)
  • **Location:** Prince of Wales/Oxford

• Open Issues
  • *Is the HP-WAN topic and problem space people want to work on?*
  • *What could the IETF do to help with these problems?*
  • *Which IETF technology is most impacted?*
  • *What are the next steps for HP-WAN discussions?*
Thank you!
Please Applaud!!! (and the crowd goes wild)
IPv6 Performance Comparison with IPv4

HotRFC Talk, IETF 120
XiPeng Xiao, v6ops co-chair
xipengxiao@gmail.com
IPv6 Performance Tests: Why

- Problem statement
  - Happy Eyeballs Protocol (HE) may mask IPv6 issues in dual stack environment by simply selecting IPv4
  - IPv6 issues not identified/solved
- Proposal
  - Test to identify/solve remaining IPv6 issues
- Benefits
  - HE will use IPv6 more → IPv6 traffic > IPv4 → migrate to IPv6-only earlier
What to Do & How to Help

- Proposed tests – open to discussion
  - DNS performance comparison
    - Is there a difference in success rate to obtain AAAA vs A record?
    - Is there a difference in latency to obtain AAAA vs A record?
      - Some DNS servers may return AAAA/A separately, so there is a possibility that the latency is different
    - Is there a difference in success rate or latency if the DNS queries are sent over IPv6 vs IPv4?
  - Connection success rate comparison
    - Is there a difference in TCP/http connection setup success rate for IPv6 vs IPv4 (e.g. between RIPE Atlas probes as sources and Alexa 100 as destinations)?
  - Connection speed comparison (when both IPv6 & IPv4 connections can be set up)
    - Is there a difference between IPv6 and IPv4 for connection setup time?
  - PLR comparison (when both IPv6 & IPv4 connections can be set up)
    - Is there a difference between IPv6 and IPv4 for packet loss rate (PLR) – the packets can be either sync/ack packets and data packets
  - Where are IPv6 packets dropped when connection failed
    - In source domain, transit network, or destination domain

- How to help
  - Design / review test cases
  - Write Python test scripts
  - Contribute test probes or credit
  - Conduct tests and report results
  - Analyze stats
  - Write report drafts
Implementing Digital Emblems on top of the DNS/DNSSEC protocol stack

HotRFC
IETF 120
Vancouver
18:00 - 20:00 PDT
Sunday, July 21, 2024

Bill Woodcock
Packet Clearing House
An **Issuer** creates **digital emblems** and cryptographically **signs** them.

**Digital emblems** are **bound** to **assets** or asset classes by **descriptions**.

**Validators** evaluate the digital **signature** which relates the **issuer** to the **digital emblem**, and the **description** which **binds** the **digital emblem** to the **asset**.
Standardized digital emblem data elements*

**Issuer**
- Visual representation: SVG / RFC9399
- Identification of law: TXT RR
- Contact information: TXT RR
- Handling flags: TXT RR
- Issuer’s signature: DNSSEC
- Third-party signatures: DNSSEC / DEP

**Asset**
- Temporal scope of validity: TIME RR
- Spatial scope of validity: LOC RR
- SI base unit of size or weight: SI RR
- WCO standardized quantity: QTY RR
- ISO 4217 currency code: CUR RR
- Names and serial numbers: TXT RR
- Distinguishing marks: TXT RR
- External references: TXT / URL

**Data at rest:**
- Zone File format

**Data in flight:**
- TLS / DANE

**In-band network response:**
- DNS, DoT

**Passive RF transponder:**
- RFID / NFC

**Active RF transponder:**
- RFID

**Active optical marking:**
- QRcode

**Active optical beacon**

**Active audio transponder**

**Active audio beacon**

**External references:**
- TXT / URL

**Issuer’s signature:**
- DNSSEC

**Third-party signatures:**
- DNSSEC / DEP

**Identiﬁcation of law:**
- TXT RR

**Visual representation:**
- SVG / RFC9399

**Validator**

**Not a complete list, but illustrative**
Thanks!
Want to talk more?
Join us in the DIEM (Digital Emblem) BoF:

09:30 - 11:30 PDT
Wednesday, July 24, 2024
Regency C/D meeting rooms

https://datatracker.ietf.org/meeting/120/materials/agenda-120-diem-01

Bill Woodcock
Packet Clearing House
woody@pch.net
Please Applaud!!! (and the crowd goes wild)
Update on the
Universal Name System (UNS)
and
Universal Certificate Authority (UCA)

Creating a global
least-trust information space
Public benefit startup, venture-backed, early stage, dual use
Least trust?

- Least attack surface
- Least knowledge
- Least authority
- Least privilege
A least-trust information space starts with

Confidential Computing

- Verified Information Space
- Verified Cryptography
- Verified Processes
- Verified Chips
Universal Name System (UNS)

A global, decentralized, automated cryptographic name system unified across all entities: people, organizations, physical things, and digital things

Universal Certificate Authority (UCA)

A global, decentralized, automated key infrastructure to solve provenance, integrity, authenticity, reputation, confidentiality, and privacy
Hierarchical, recursive, chip-level, process-level attestation and verification
+ decentralized identifiers and automated pairwise cryptography
Globally verified
Fully automated

Quantum-resistant
No insider at all

Humans
Orgs

Bits
Things

ENTITY A
ENTITY B
## Information Isolation

Each process has its own encrypted information space.

<table>
<thead>
<tr>
<th>Cell Number</th>
<th>Cell content, encrypted with Cell Key</th>
</tr>
</thead>
<tbody>
<tr>
<td>pZztwZxRTD2zchikuouOUEj6c24z+e+p3zkfcF0jzh/lq/KqubVb5S0x0ttZqyxP6h/lOzXyfg82Z2</td>
<td>vvuiPYJ/PRwPQV8BkboWSHIhmVYoZI1MvyI/pTtwru=</td>
</tr>
<tr>
<td>i/S0ov4KRZDmQftjoDREDplIqtybopet/pUppVTHQ7YyvAuuOcrlYDPWmqTaUHqaq3P+/+</td>
<td>ia/II7n5+SwWldp6+P8UJdh2xXZ/z/VyN9vcpaTXyre=</td>
</tr>
<tr>
<td>NMBOBIR704ZcKtIus/nvuZvckZOM1uxIab/A/KcJ7/kgrokklIpe2M9M9x5bn09Y0stx4jzXHD</td>
<td>wt2NF+xToCogaMzfrFmRO4075hJs/HnbjRu3/iJmV0=</td>
</tr>
<tr>
<td>ANcu66m2zXf9trm3cFpuck0ARymweiBILwkzHCRjBпов=</td>
<td>ANCuO62zxmXf9trm3cFpuk0ARymweiBILwkzHCRjBпов=</td>
</tr>
<tr>
<td>PfNtwz2YKOBfMomykl/1xLwbybhu4TICj3yHh/rz/uzmNRKXuiCaeIWGUULUThauUkIum0Gsm3Zrt</td>
<td>4osTde7TTrnFSlq?nbsm5sDjkh66q1utd8Kn2uEp3E41=</td>
</tr>
<tr>
<td>4s2Tvzyh7ujnQm8h1h7j3y2S3X5675VwNg8g4kXfMc2XhLC62cXh959t6</td>
<td>8IEV3Rj/NupWetEEif/FNeumi+tSmsOrj04xav/76iwWgjU02RS3Bkkeuruq3CQpcGxwCzTRawWgV4k</td>
</tr>
<tr>
<td>YC5SMWz7JnAqggyZf4x4bB0o0BCJp+0nm/M3o0DyCrn11+cQtbF0Y8S7ty/ZyNg6NwosMufenKQW</td>
<td>LKIE74W6Z6jwwuULfhnWS2ZHz4q4x2zA0YvC/5DCd8k=</td>
</tr>
<tr>
<td>jb++Rf6vd/A+k+I+T+Epmq4wZzRqzy7yxtsT4m9HnbA3NAmCen11Nnxr7FyB3DHsOxVhdsWnDxO</td>
<td>cWFSsuyhk6D6ntTfkwrRc+DzStktwRaQ1k5S0hx4=</td>
</tr>
<tr>
<td>j+k+BcEaDc0TGcPwDFTCw303b30m3930c75kn91w9Kn4c+cj2ybTkxO3FDCyWdS65o202w</td>
<td>xDrknz16bNaYm5x7QwQGmwKQzJhAXsYv/1o+Dizc7BaO9Q5sv/FLTsWT1avDVG5178Cwbeee1GMg</td>
</tr>
<tr>
<td>SAPP4ppvWwd+du9ALPnAfcd01ILiZcF/FFqv60j3ptSh2F8myM7Stth2PX0w1n8j80wn9</td>
<td>6WUN0b/7hcb0o0M3y5ns8YhDwVCxYqTq470FvFU44eEmK+FQEc/4rCp+5zvBq7w14dEoA0x2</td>
</tr>
<tr>
<td>2HfH0E0vKgVFsDStpI26DnvDvPqehkPeg6e0/9r9X6GmC9co9s3FwpxorXVH7+2P8xKwz130n9</td>
<td>VxwoLnn1RgDQ7trCurXh4lA3Df5oNMe0He02c5Lx7SOZ=</td>
</tr>
<tr>
<td>5Gy6hknLxLy76icyKu39j3tDFqy1+TVB4ac.FH73hav0mYezYe1H53N3u4CfYhj pervYGUCJy3JQEU8b</td>
<td>+74cDUzzOTUI0u3cGyEUG2BgcwVsg0AM8sdd0Tg</td>
</tr>
</tbody>
</table>
Process isolation is not sufficient

Processes come and go. They need to persist and secure their own information space outside their isolated computing environment, without having to trust an external system.

Information isolation is necessary

Conventional identifiers require processes to trust what's outside their isolation boundaries. Cryptographic identifiers enable each process to mathematically secure its own information space.
Side Meeting in **Prince of Wales/Oxford** on **Wed @ 13:00**

**UNS / UCA overview and updates** since IETF 119, and **conversation**

Figure out **how to bring this work to the IETF**

**Discuss collaboration and coalition** for neutral governance

manu@hushmesh.com
Please Applaud!!! (and the crowd goes wild)
GREEN BOF Update: Moving Toward Energy Efficiency Network Management

Qin Wu (bill.wu@huawei.com)
Background and Motivation

• Power management widely adopted in the past for enterprise networks
  • E.g., Monitor power consumption of HVAC in the smart building automation
  • Monitor power consumption of IT device such as personal computers, wireless access points, network switches in the campus network

• With the rapid development of network technology such as 5G, AI computing, high speed ethernet, etc and explosive growth of network traffic,
  • The network capacity and sites are continuing to increase which also drive tremendous growth in equipment energy consumption costs.
    • 85% (Network ) 5% (Terminal) 10% (Office)
    • Data Center (20~25%), Mobile Wireless (45~60%)
  • In the meanwhile, a large proportion of the vast amounts of energy consumed is unnecessarily wasted.
Challenges and Goal

• Network operators are seeking for automation tools and solutions to better assess and control the energy consumption of networks, devices, and devices/components across their networks.
  • The focus of targeted devices are the ones consuming most of energy
    • E.g., pure network element in mobile network or fixed network
    • Hybrid scenario such as Power supply(e.g., PDU)+ network elements in data center Network
  • Use cases such as
    • Network visibility to energy consumption per device, per component, energy efficiency per device, per component,
    • Power usage effectiveness measurement on the whole data center network, etc

• Power Consumption monitoring on devices is not sufficient since
  • Monitoring only tell you how much power are consumed at specific device.
  • But doesn’t tell you when where to consume such power, why consume so much power and how to save the power.

• Technology trend is moving from power consumption monitoring toward energy efficiency observability and management
  • Global visibility to network topology data, capability inventory data, power data, energy data since
    • Mapping or correlation between data at component level, device level and network level modelled data are visible
    • Allow optimizing energy use on network devices based on capability while improving the overall network utilization
The GREEN BOF Introduction

• The GREEN BOF is WG forming BOF
  • Aim at creating a new WG
  • Tackle complexity of energy management world and address these challenges faced by today’s network operators
  • Explore the information to be exposed in the YANG model and the requirements for energy efficiency management

• GREEN BOF Charter Proposal:
  • https://datatracker.ietf.org/group/green/about/

• BOF Meeting Time and Location:
  • Wednesday afternoon, 1st session
  • Location: Regency C/D

• The mailing list: green-bof@ietf.org

• Your input on AD’s question in chairs slides are welcome!
Please Applaud!!! (and the crowd goes wild)
Introducing the SecureDrop Protocol

IETF 120
Giulio Berra • Freedom of the Press Foundation
SecureDrop today: architecture

OpenPGP encryption at rest

Tor encryption in transit
E2EE SecureDrop: goals

- Use modern end-to-end encryption
- Do not require file or information persistence on the source/whistleblower side
- Ensure system architecture does not preclude deployment in a hostile, potentially compromised environment
- Avoid, minimize, and hide metadata from the server
E2EE SecureDrop: non-goals

- High volume, high traffic
- Low latency
- Arbitrary-sized groups
- Arbitrary direct messages
- Federation
E2EE SecureDrop: properties

1. No accounts, and therefore no user authentication
2. No message flow metadata
3. No changes in server state are observable externally
4. No ciphertext collection or information leaks
## Comparison of E2EE messaging protocols

<table>
<thead>
<tr>
<th>Approach</th>
<th>Primitives Library</th>
<th>Peer-reviewed Library</th>
<th>Groups</th>
<th>Scalable</th>
<th>Concealed Recipient</th>
<th>Private Server State</th>
<th>Avoids Accounts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signal</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Trial Decryption</td>
<td>Yes</td>
<td>N/A(^1)</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Oblivious Message Retrieval</td>
<td>No</td>
<td>No</td>
<td>Yes(^2)</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>SecureDrop Protocol</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No(^3)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

1. While there isn’t a single standard library, the implementation is straightforward.

2. *New iteration of the research focuses on groups.*

3. SecureDrop Protocol does not preclude scalability, but scaling to mass adoption level (i.e. millions of users) is a [nonrequirement](https://securedrop.org) for our purposes.
E2EE SecureDrop: high-level flow

Sender → SD Server

payload, clue → Remixed Clues

SD Server → Recipient

Payload ID → Payload

Trial decryption on all remixed clues to discover payload ID, payload decryption
E2EE SecureDrop: follow-up questions

- Most whistleblowing software/services have a similar setup: web-based and single server
- Could a stable, maintained library improve the ecosystem? Even the commercial ones?
- Is the threat model accurate, realistic, and broad enough?
- Is the protocol portable in a PQ world? (3-party commutative DH is not trivial)
- What other countermeasures are needed? Decoy/noise traffic?
Acknowledgments and ongoing work

- **Preliminary cryptographic audit** done by Michele Orrù (French National Center for Cryptographic Research/CNRS)
- **Formal analysis** in progress by Luca Maier supervised by Felix Linker (Swiss Federal Institute of Technology/ETH Zürich)
- **Funded** by the Filecoin Foundation for the Decentralized Web
Our ask: your feedback

Read more:

- https://github.com/freedomofpress/securedrop-protocol

Write to us:

- giulio@freedom.press (or Signal: giulio.99)
- cory@freedom.press (or Signal: cfm.38)
Please Applaud!!! *(and the crowd goes wild)*
THANK YOU
SEE YOU AT 121!