IETF 121 HotRFC

Sunday 3 November 2024

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/(Privacy Policy)

Note Really Well

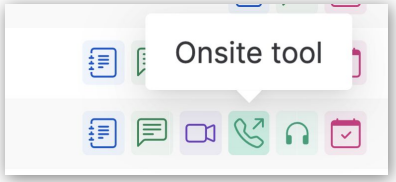
- IETF meetings, virtual meetings, and mailing lists are intended for professional collaboration and networking, as defined in the IETF Guidelines for Conduct (RFC 7154), the IETF Anti-Harassment Policy, and the IETF Anti-Harassment Procedures (RFC 7776). If you have any concerns about observed behavior, 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.

This session is being recorded

IETF 121 Meeting Tips

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.

Resources for IETF 121 Dublin

- Agenda
  https://datatracker.ietf.org/meeting/agenda
- Meetecho and other information:
  https://www.ietf.org/how/meetings/preparation
- If you need technical assistance, see the Reporting Issues page:
  http://www.ietf.org/how/meetings/issues/

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)

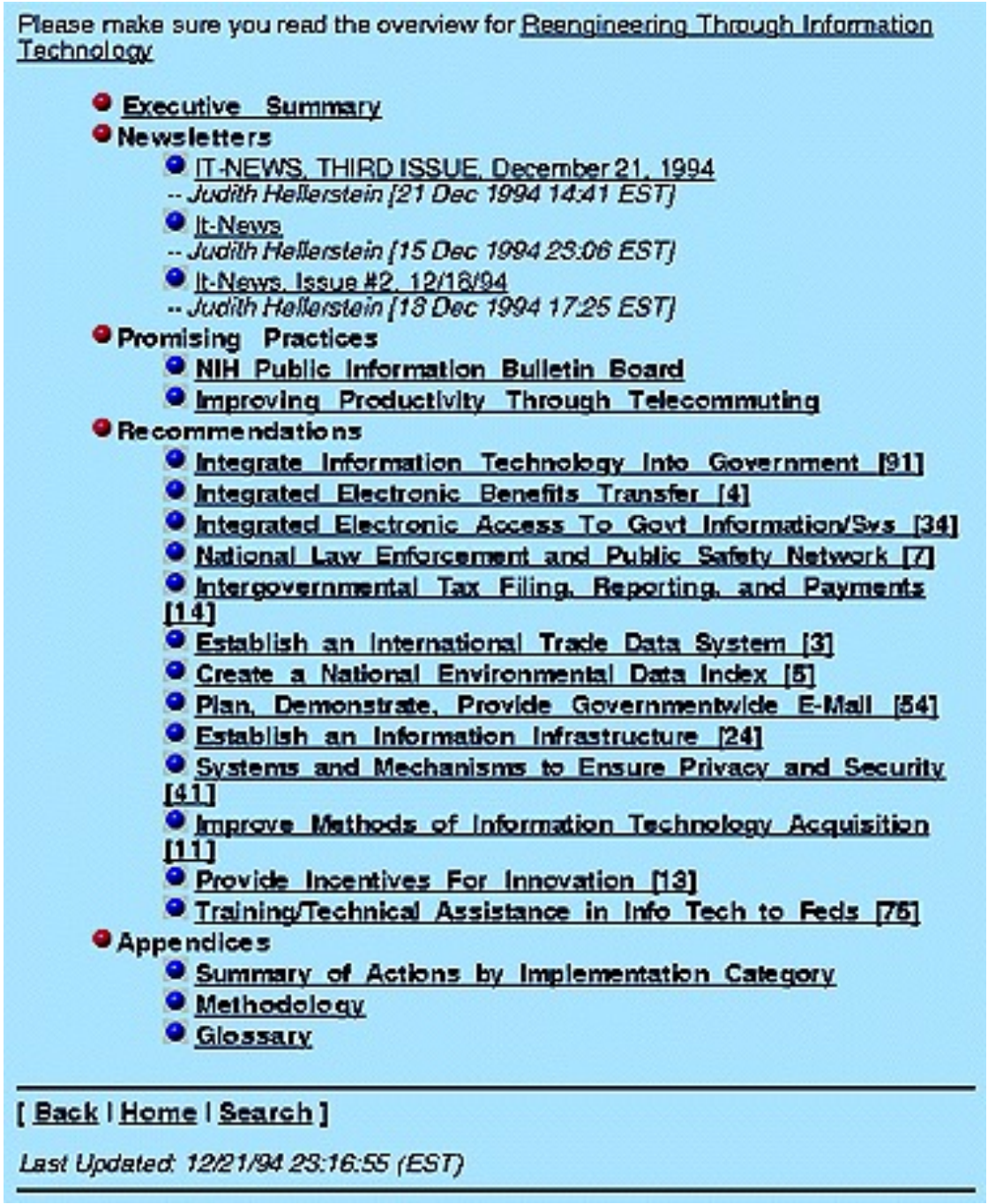
Palimpsest

Structured Collaborative Editing

Phillip Hallam-Baker

The Open Meeting
(Mallery & Hurwitz)

- A Part of Vice President Al Gore's National Performance review
  - Introduced tagged semantics
  - Required a LISP machine to run



Please make sure you read the overview for Reengineering Through Information Technology

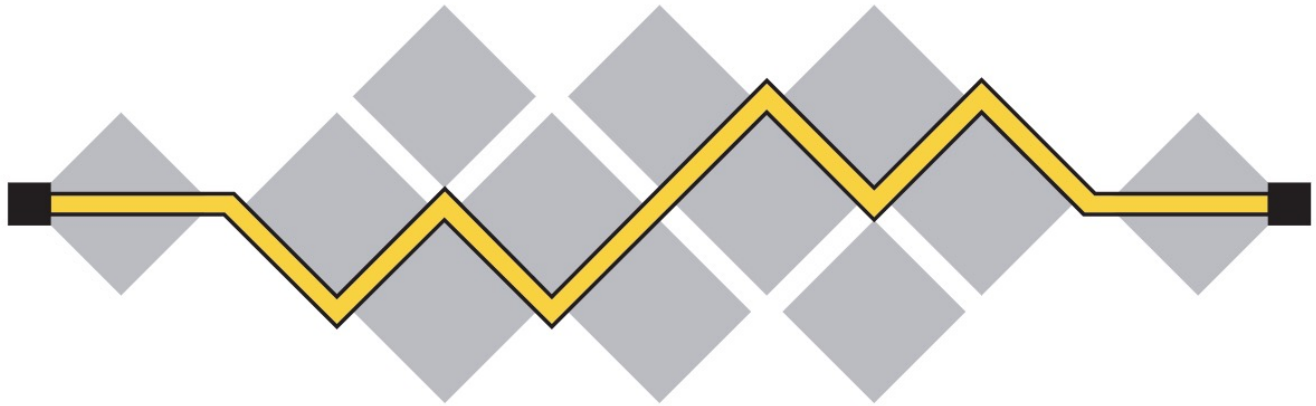
- Executive Summary
- Newsletters
  - IT-NEWS, THIRD ISSUE, December 21, 1994
    -- *Judith Hellerstein [21 Dec 1994 14:41 EST]*
  - It-News
    -- *Judith Hellerstein [15 Dec 1994 23:06 EST]*
  - It-News, Issue #2, 12/16/94
    -- *Judith Hellerstein [18 Dec 1994 17:25 EST]*
- Promising Practices
  - NIH Public Information Bulletin Board
  - Improving Productivity Through Telecommuting
- Recommendations
  - Integrate Information Technology Into Government [91]
  - Integrated Electronic Benefits Transfer [4]
  - Integrated Electronic Access To Govt Information/Svs [34]
  - National Law Enforcement and Public Safety Network [7]
  - Intergovernmental Tax Filing, Reporting, and Payments [14]
  - Establish an International Trade Data System [3]
  - Create a National Environmental Data Index [5]
  - Plan, Demonstrate, Provide Governmentwide E-Mail [54]
  - Establish an Information Infrastructure [24]
  - Systems and Mechanisms to Ensure Privacy and Security [41]
  - Improve Methods of Information Technology Acquisition [11]
  - Provide Incentives For Innovation [13]
  - Training/Technical Assistance in Info Tech to Feds [75]
- Appendices
  - Summary of Actions by Implementation Category
  - Methodology
  - Glossary

[Back | Home | Search]

Last Updated: 12/21/94 23:16:55 (EST)

The Draft

localhost:15099



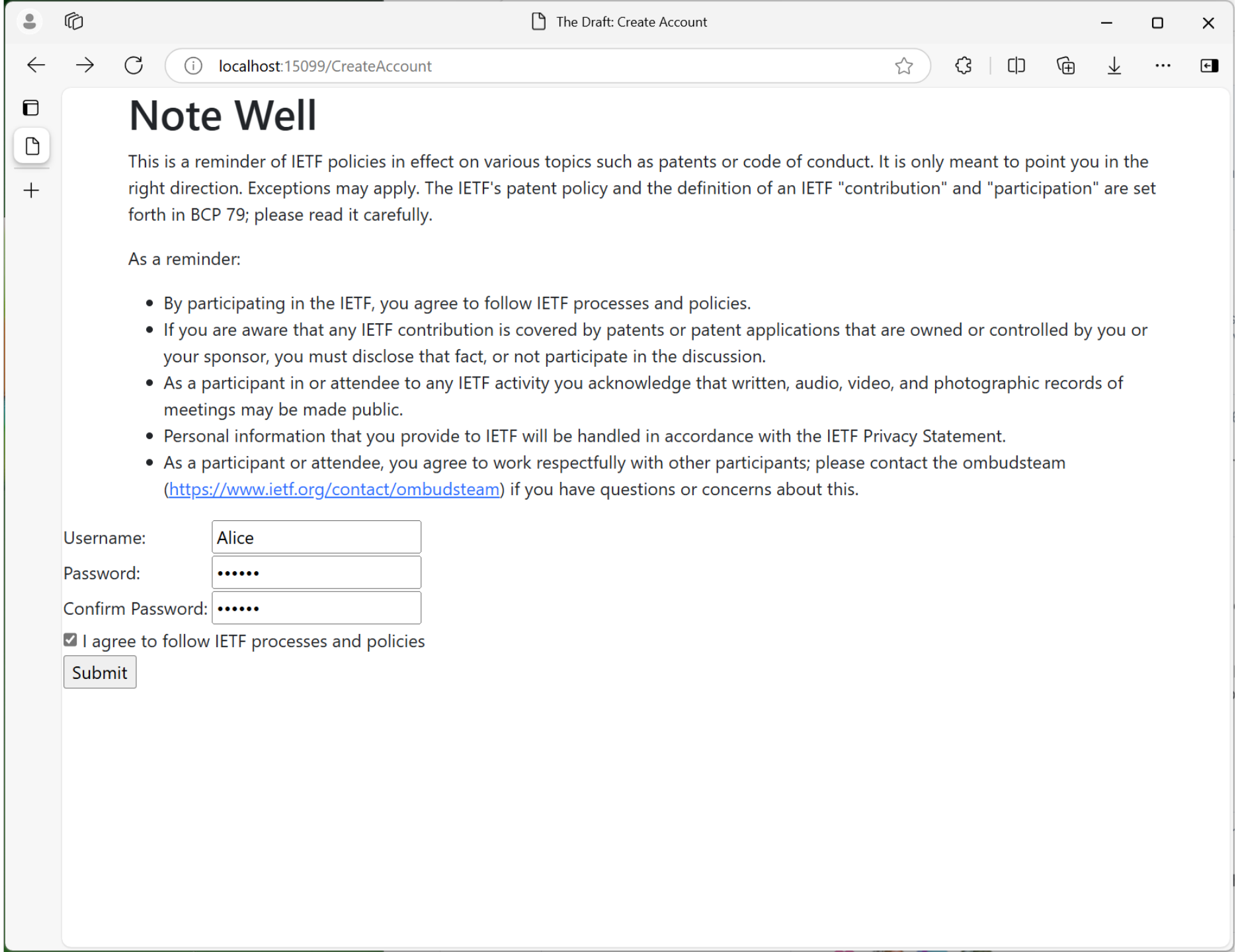
I E T F®

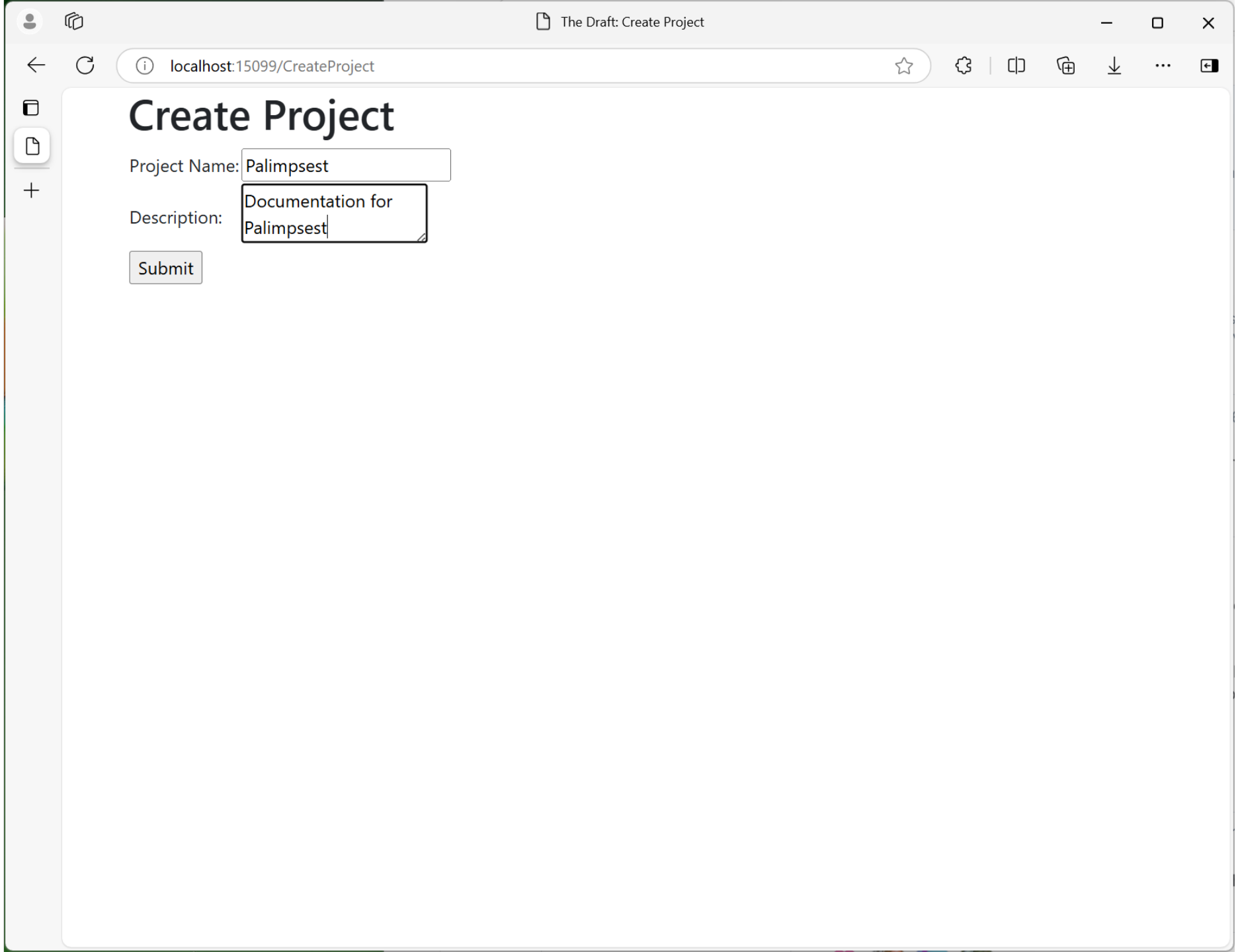
Home The Draft

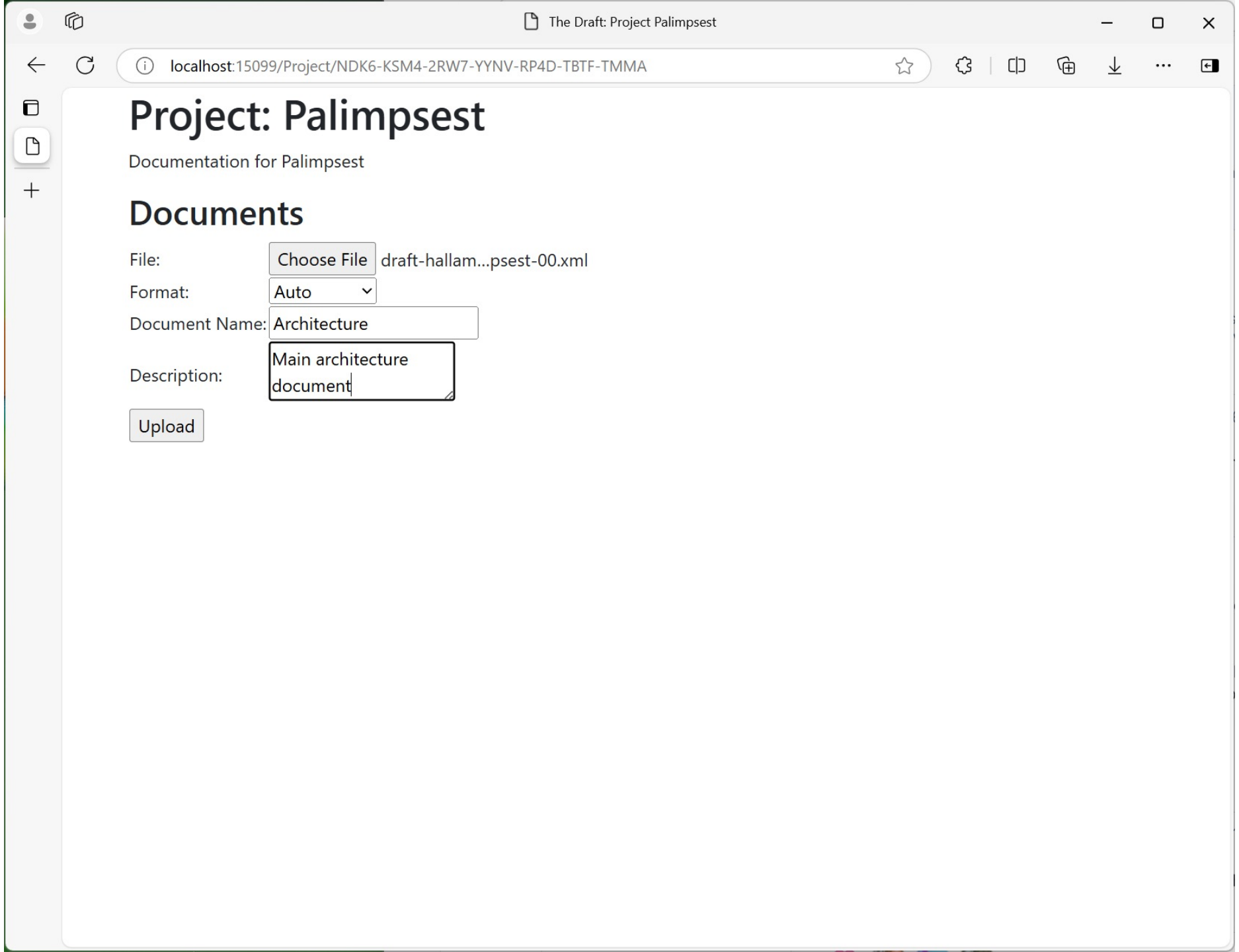
Sign In

Create Account

Create Project


The Draft: Create Account
localhost:15099/CreateAccount
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.
Username:
Alice
Password:
Confirm Password:
I agree to follow IETF processes and policies
Submit


The Draft: Create Project
localhost:15099/CreateProject
Create Project
Project Name: Palimpsest
Description: Documentation for Palimpsest
Submit


The Draft: Project Palimpsest
localhost:15099/Project/NDK6-KSM4-2RW7-YYNV-RP4D-TBTF-TMMA
Project: Palimpsest
Documentation for Palimpsest
Documents
File:
Choose File
draft-hallam...psest-00.xml
Format:
Auto
Document Name:
Architecture
Description:
Main architecture document
Upload

Workgroup:
Network Working Group

Stream:
Internet-Draft

Intended status:
Informational

Published:
31 October 2024

ISSN:
2070-1721

Expires
4 May 2025

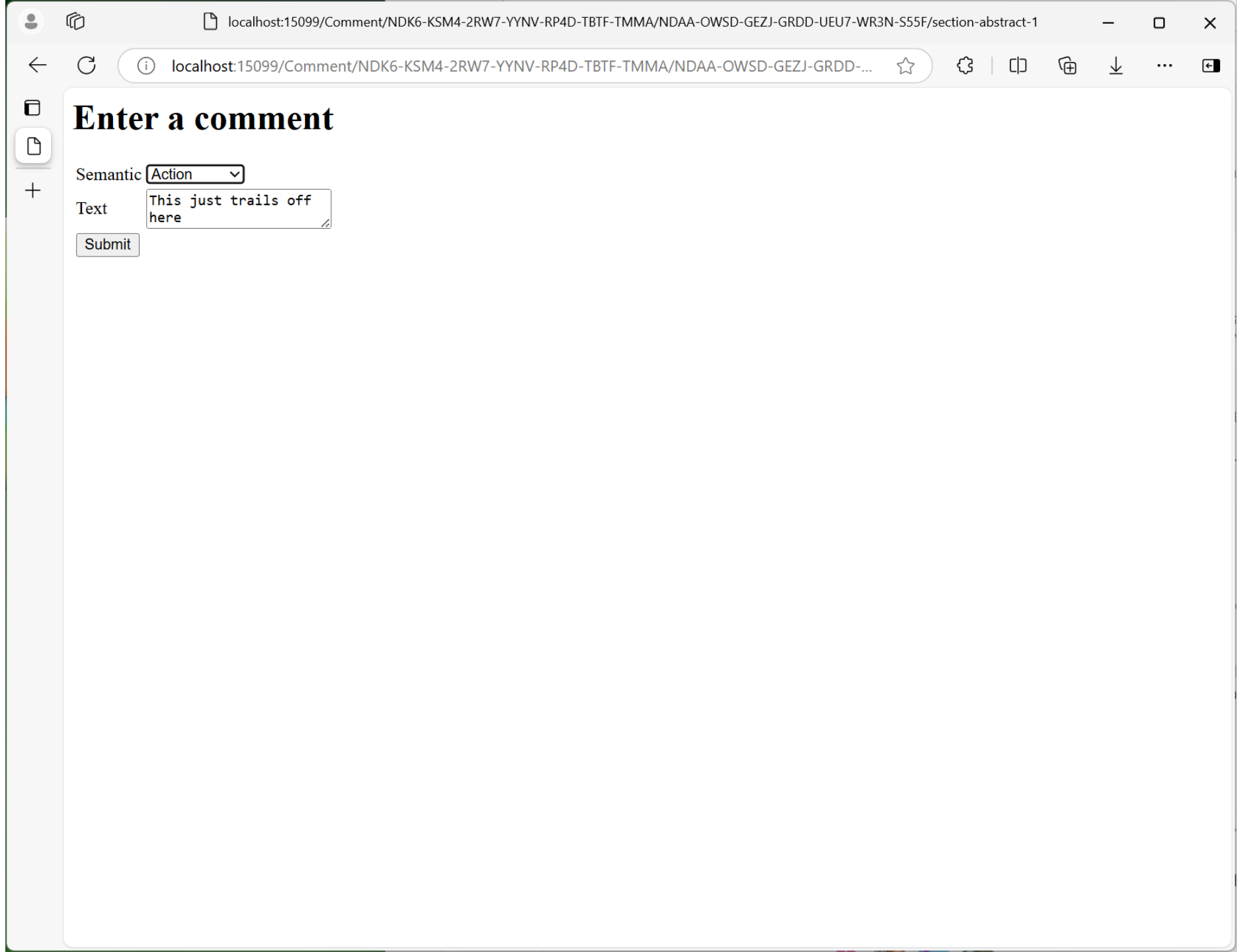
Authors:
Phillip Hallam-Baker
ThresholdSecrets.com

Palimpsest

Abstract

This document provides an overview of the Palimpsest structured collaboration system. Palimpsest facilitates review of documents through reactions tagged with weak semantics defining processing steps for the reaction. Documents are grouped into projects with a common set of allowed semantic moves and processing steps. This allows the revie

Status of This Memo


localhost:15099/Comment/NDK6-KSM4-2RW7-YYNV-RP4D-TBTF-TMMA/NDAA-OWSD-GEZJ-GRDD-UEU7-WR3N-S55F/section-abstract-1
localhost:15099/Comment/NDK6-KSM4-2RW7-YYNV-RP4D-TBTF-TMMA/NDAA-OWSD-GEZJ-GRDD-...
Enter a comment
Semantic
Action
Text
This just trails off here
Submit

Palimpsest §title

Abstract §abstract

This document provides an overview of the Palimpsest structured collaboration system. Palimpsest facilitates review of documents through reactions tagged with weak semantics defining processing steps for the reaction. Documents are grouped into projects with a common set of allowed semantic moves and processing steps. This allows the revie¶ §section-abstract-1

[Alice] **action**: This just trails off here

Status of This Memo §n-status-of-this-memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.¶ §section-boilerplate-1-1

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.¶ §section-boilerplate-1-2

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time.It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."¶ §section-boilerplate-1-3

This Internet-Draft will expire on May 4, 2025¶ §section-boilerplate-1-4

Copyright Notice §n-copyright-notice

Table of Contents §toc

Semantic Traces

- Internal
  - Question → Answer → Agree → Closed
  - Text → Agree → Closed
- Raise Issue
  - Question → Answer → Issue
  - Information → Issue
  - Issue
- Publish
  - Approve

Why not Github?

- Github is designed for collaboratively editing code
  - Documents are not code
  - Using a ‘Pull request’ to propose an alternative is a hack
    - Try doing it from an iPad

- Palimpsest ties comments to documents
  - Distinguish nits from issues
  - Can download document source in Word, Markdown or XML

Next Steps

- Extend engineering prototype
  - Install Bootstrap style sheet
  - Moderation interface
  - Report generation
  - Email subscription
  - [Client for zero-trust / End to End secure hosting mode]

- Trial?

Please Applaud!!! (and the crowd goes wild)

Large Language Models (LLMs) for Networking

Mingzhe Xing
Beijing Zhongguancun Laboratory
xingmz@zgclab.edu.cn

Background & Motivation

- **Network Challenges:**
  - Complex environments
  - Diverse demands
  - Rapid iteration cycles
- **LLMs' Emerging Capabilities:**
  - Concept Understanding
  - Logical Reasoning
  - Tool Utilization

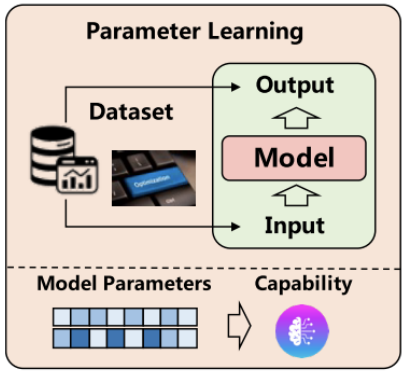
Based on Hypothesis

$QoE = \alpha*\log(R) - \beta*\log(D) - \gamma*\log(C)$

R: Resolution
D: Delay
C: Change rate

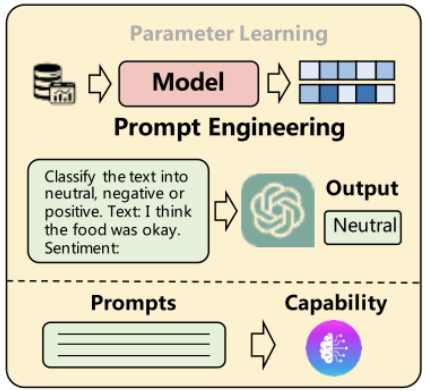
Modeling

Domain dataset

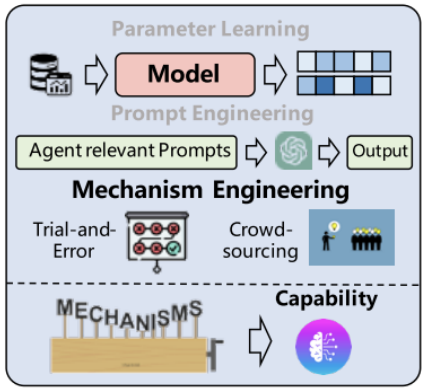


ML

Extensive datasets and Large-scale parameters



LLM



LLM Agent

Increased Attention on LLMs for Networking

- **HotNets 2023**
  - November 2023 @ MIT
  - Two sessions (2 out of 9) are dedicated to this topic.

Session 6: Can LLMs Manage Networks?
Session Chair: Nate Foster (Cornell)

Adapting Foundation Models for Operator Data Analytics
Manikanta Kotaru (Microsoft)

A Holistic View of AI-driven Network Incident Management
Pouya Hamadanian (Microsoft Research, MIT); Behnaz Arzani, Sadjad Fouladi, Siva Kesava
Rodrigo Fonseca (Azure Systems Research); Denizcan Billor, Ahmad Cheema, Edet Nkposo
(Microsoft Research)

What do LLMs need to Synthesize Correct Router Configurations?
Rajdeep Mondal, Alan Tang (UCLA); Ryan Beckett (Microsoft Research); Todd Millstein, Ge

Enhancing Network Management Using Code Generated by Large Language Models
Sathiya Kumaran Mani (Microsoft); Yajie Zhou (Microsoft and Boston University); Kevin Hs
Segarra (Microsoft and Rice University); Trevor Eberl, Eliran Azulai, Ido Frizler, Ranveer Ch

HotNets 2023: Twenty-Second ACM Workshop on Hot Topics in Networks

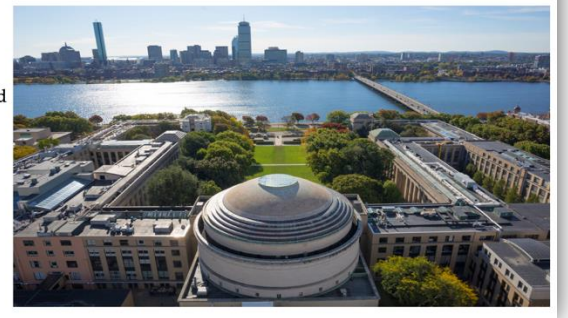
November 28-29, 2023 — Cambridge, Massachusetts, USA

Overview

The Twenty-second ACM Workshop on Hot Topics in Networks (HotNets 2023) will bring together researchers in computer networks and systems to engage in a lively debate on the theory and practice of networking. HotNets provides a venue for discussing innovative ideas and for debating future research agendas in networking.

Location

Samberg Conference Center
50 Memorial Dr, Cambridge, MA 02142
6th floor, Dinning Room 5 & 6
MIT



Session 2: Can LLMs reason about networking problems, and their solution?
Session Chair: Ranjita Bhagwan (Google)

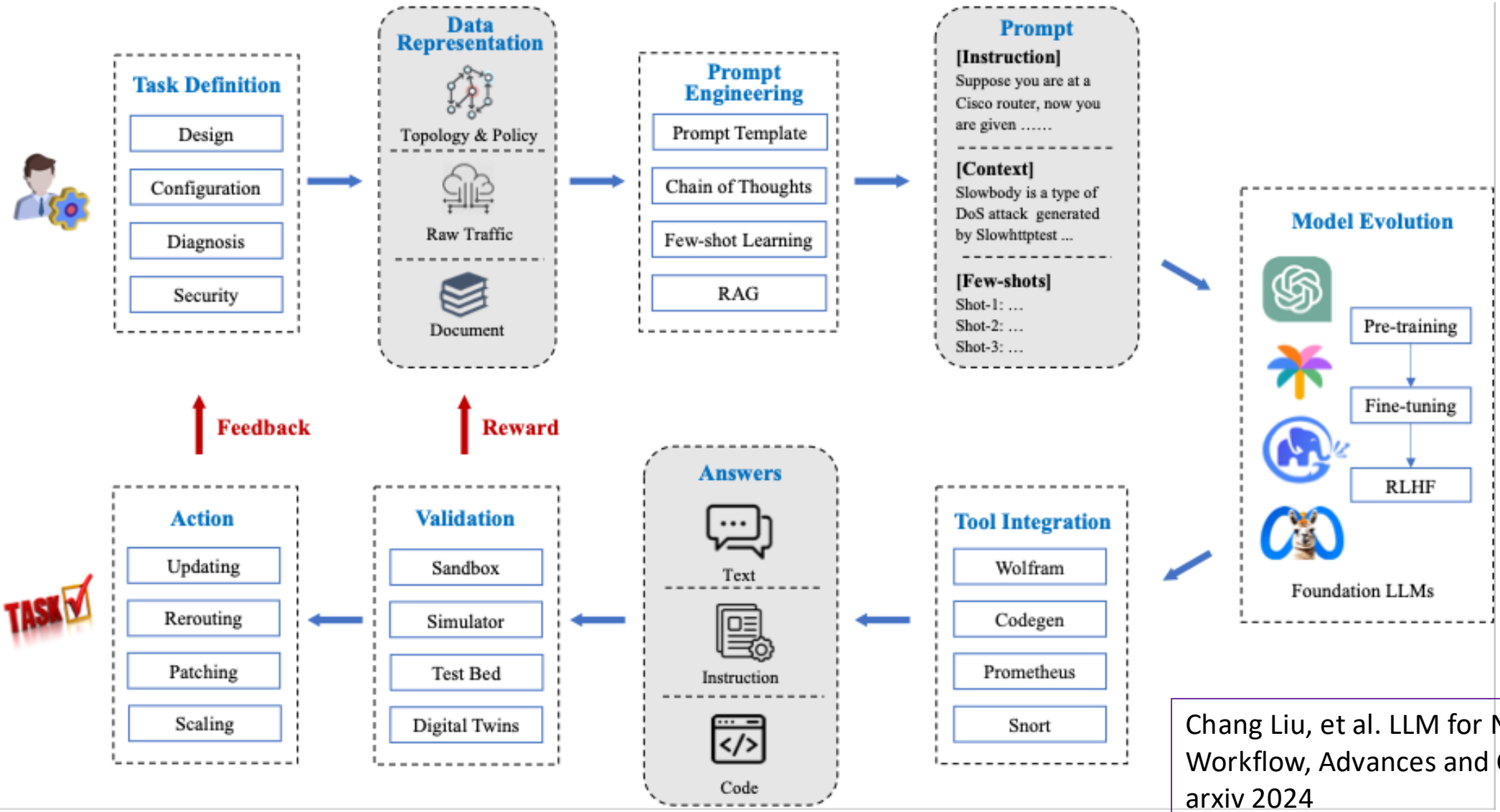
Towards Interactive Research Agents for Internet Incident Investigation
Yajie Zhou, Nengneng Yu (Boston University); Zaoxing Liu (University of Marylanc

PROSPER: Extracting Protocol Specifications Using Large Language Models
Prakhar Sharma, Vinod Yegneswaran (SRI International)

Towards Integrating Formal Methods into ML-Based Systems for Networking
Fengchen Gong, Divya Raghunathan, Aarti Gupta, Maria Apostolaki (Princeton Un

Toward Reproducing Network Research Results Using Large Language Models
Qiao Xiang, Yuling Lin, Mingjun Fan, Bang Huang, Siyong Huang, Ridi Wen (Xiam
Kong (Shanghai Jiao Tong University, China); Jiwu Shu (Xiamen University)

Workflow for applying LLMs in Networking



Chang Liu, et al. LLM for Networking: Workflow, Advances and Challenges. arxiv 2024

Challenges and Future Directions

- **Understanding Multimodal Data**
  - Multimodal data plays a critical role in the networking domain
- **Prompt Engineering for Deliberate Reasoning**
  - Many networking tasks involve integrating multiple intermediate results to reach a final conclusion
  - multi-path reasoning processes, e.g., Tree of Thoughts or Graph of Thoughts
- **Network-specific LLMs**
  - Construct LLMs specialized for the networking domain to enhance efficiency and performance
- **Validation Environment**
  - Ensuring the reliability and safety of applying LLMs in networking presents a critical challenge

Thanks

Mingzhe Xing
Beijing Zhongguancun Laboratory
xingmz@zgclab.edu.cn

Please Applaud!!! (and the crowd goes wild)

KIRA – Scalable Zero-Touch Routing

KIRA: Kademlia-directed ID-based Routing Architecture

Karlsruhe Institute of Technology

Contact:
bless@kit.edu

- Scalability: 100,000s of nodes (in a single domain)
- Zero-touch: no configuration required
- Goal: provide highly resilient autonomous control plane connectivity
- Need this in every networked device → IETF Standard
- Internet-Draft: https://datatracker.ietf.org/doc/draft-bless-rtgwg-kira/
  - Comments welcome!
  - Running code provides zero-touch IPv6 connectivity

More Info

https://s.kit.edu/KIRA

- Looking for: collaborations toward BoF & implementers
- Side meeting/BarBOF:
  Wednesday Nov 6th, 19.00–20.00h, Wicklow Meeting Room 4
  - Q&A, collaboration

Please Applaud!!! (and the crowd goes wild)

Update on the

Universal Name System (UNS) and **Universal Certificate Authority (UCA)**

About Extrinsic, Intrinsic, Decentralized, and Stem Identifiers

A new type of identifiers

for complex digital entities

Entities need inherent

individuality, authenticity, history, and relationships

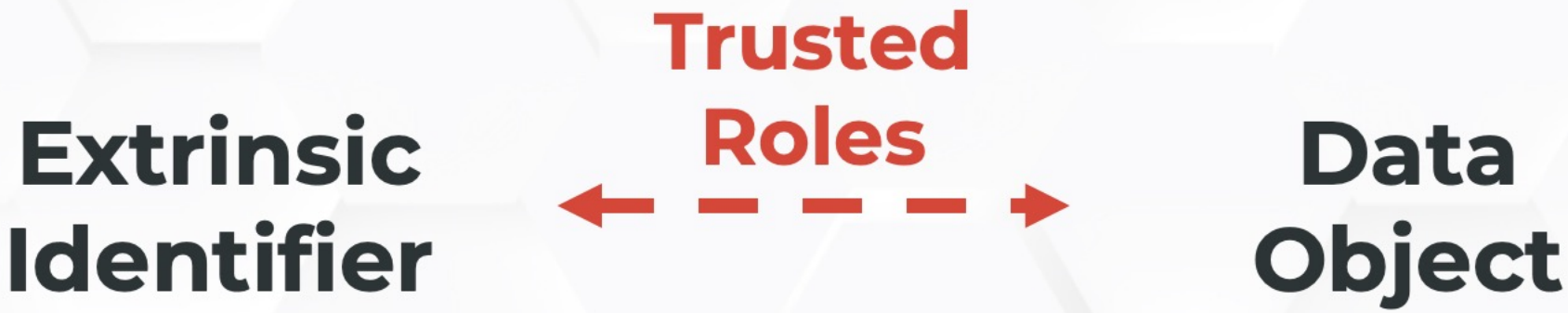
Requires assurance of provenance, integrity, and confidentiality

for data objects across distributed systems

Why bring it to IETF?

Pretty much everything is a complex digital entity,
with its **own lifecycle and relationships** with other entities

People, organizations, chips, IoT devices, code snippets,
executables, workloads, any item in any supply chain...



Identifier persists when data object changes but requires trust, undermines integrity and confidentiality

Mathematical integrity but

identifier changes when data object changes

+ Public-Private Key Pairs
(Trusted roles)

Decentralized Identifier  **Data Object**

Mathematical integrity but

assumes secure key management without verifiability

+ Trusted Execution Environments

Stem Identifier  **Data Object**

Mathematical integrity and verifiability,

enables “stemcryption” for provenance and confidentiality

Stem Identifier (StemID)

Random 256-bit with full entropy

Exclusively generated and managed in TEEs

Identifier AND key simultaneously

c1KXzxfVRf1JlJYVKq4zMGixUBGOF3J4LRrDHeJxpHk

“Stemcryption”

Encryption with keys derived from a StemID

or with keys themselves stemcrypted

Entity StemID **#** relationship_string **#** keyname_string

is the HMAC function

symmetric signature *and* key derivation function

Universal Name System (UNS)

A global, decentralized, automated, verified cryptographic name system

unified across all types of entities: people, organizations, physical things, and digital things

Universal Certificate Authority (UCA)

A global, decentralized, automated, verified key infrastructure

to solve provenance, integrity, authenticity, reputation, confidentiality, and privacy

Side Meeting in **Wicklow Meeting Room 4 (WMR4)** on **Mon @ 13:30**

UNS / UCA overview and **updates** since IETF 120, and **conversation**

Discuss collaboration and coalition for neutral governance

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

manu@hushmesh.com

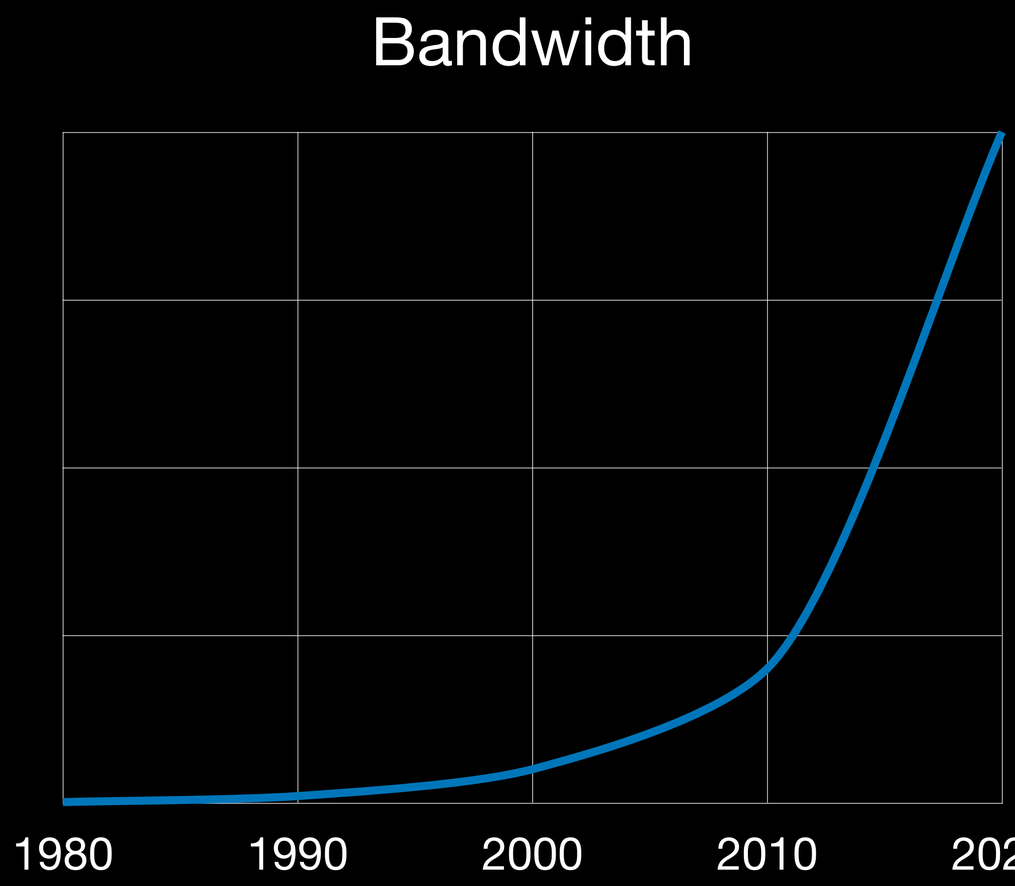
Please Applaud!!! (and the crowd goes wild)

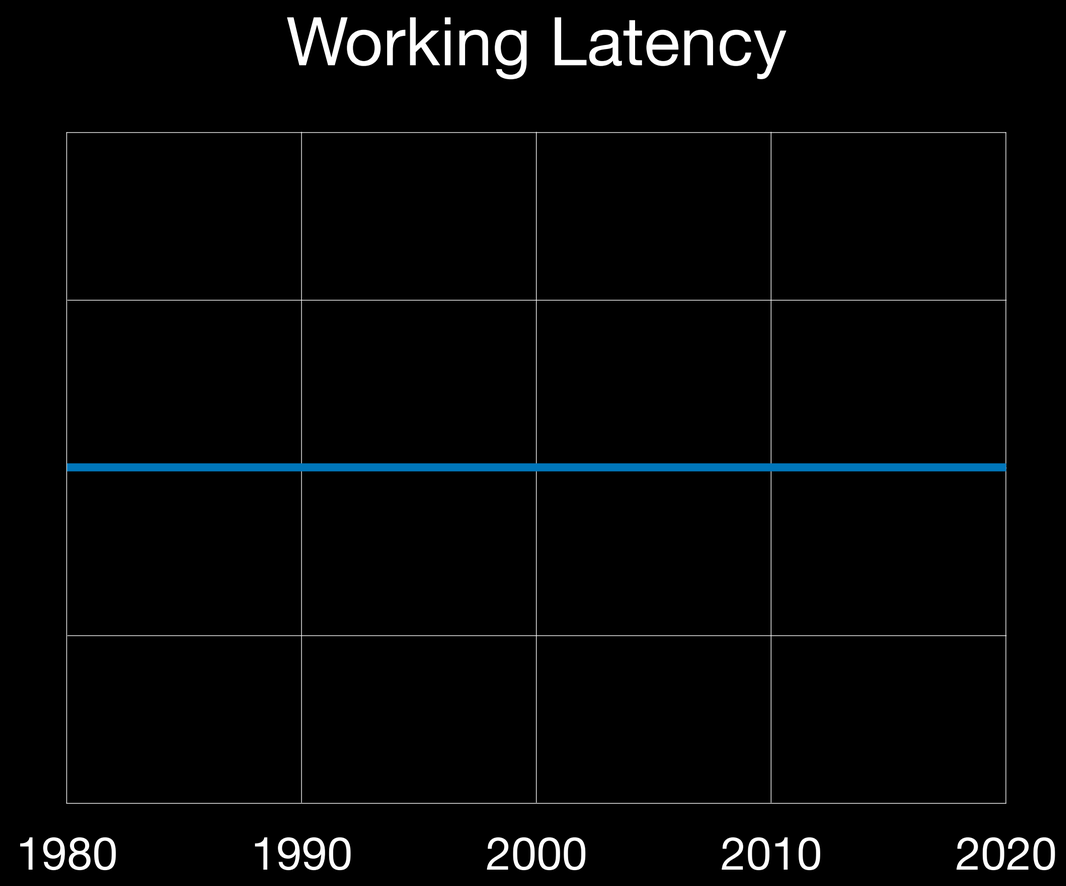
Roundtrips Per Minute (RPM)

HotRFC, IETF 121 Dublin, November 2024

Stuart Cheshire, Apple

Bandwidth and Latency





Why has Working Latency stagnated?

Engineers improve what they can measure

- Lots of tools measure throughput
- We measure latency badly — only on idle networks

Bufferbloat is still common

We still accept videoconferencing glitches

New Latency Measurement Tool
Roundtrips Per Minute (RPM)

Measures latency while network is used, not when it is idle

Reports responsiveness — reciprocal of latency

- Latency, measured in time (e.g., milliseconds)
- $^{1}/_{\text{latency}}$ gives frequency (Hz)
- Multiply by 60 to get Roundtrips Per Minute (RPM)
- Typical result reported as three-digit or four-digit integer
- Bigger numbers are better

Call to Videoconferencing Engineers

and other delay-sensitive applications

Is our RPM test measuring the delay properties you care about?

- 90th percentile delay? 95th percentile? 99th percentile?

Reading: draft-ietf-ippm-responsiveness

Discussion: IPPM meeting, 13:00 - 15:00 Monday

Please Applaud!!! (and the crowd goes wild)

Formal Analysis of Attested TLS for Confidential Computing

Muhammad Usama Sardar

TU Dresden, Germany

November 3, 2024

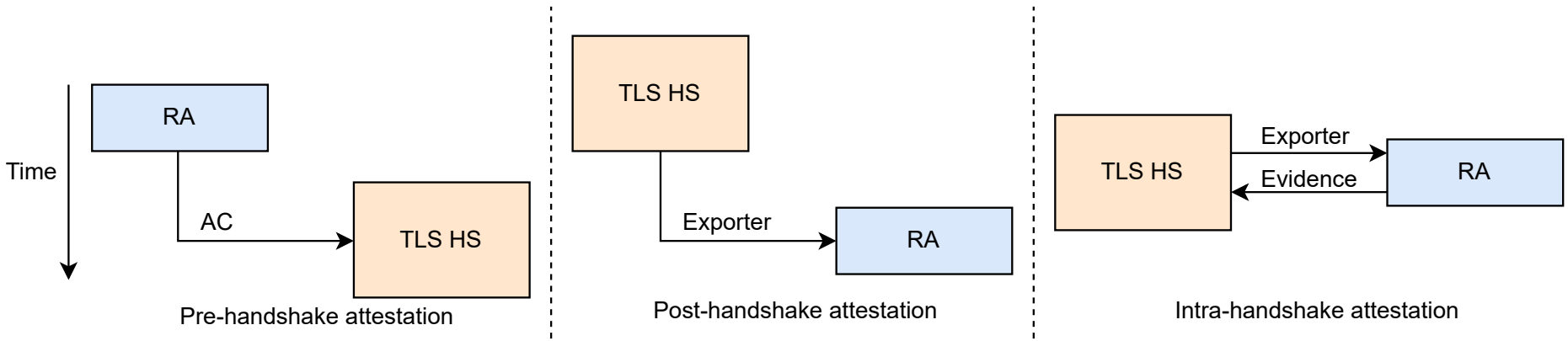
Attested TLS

- TLS 1.3[1]
  - Good for network security
  - Not good for endpoint security
- Use case: Confidential Computing

[1] https://datatracker.ietf.org/doc/html/rfc8446

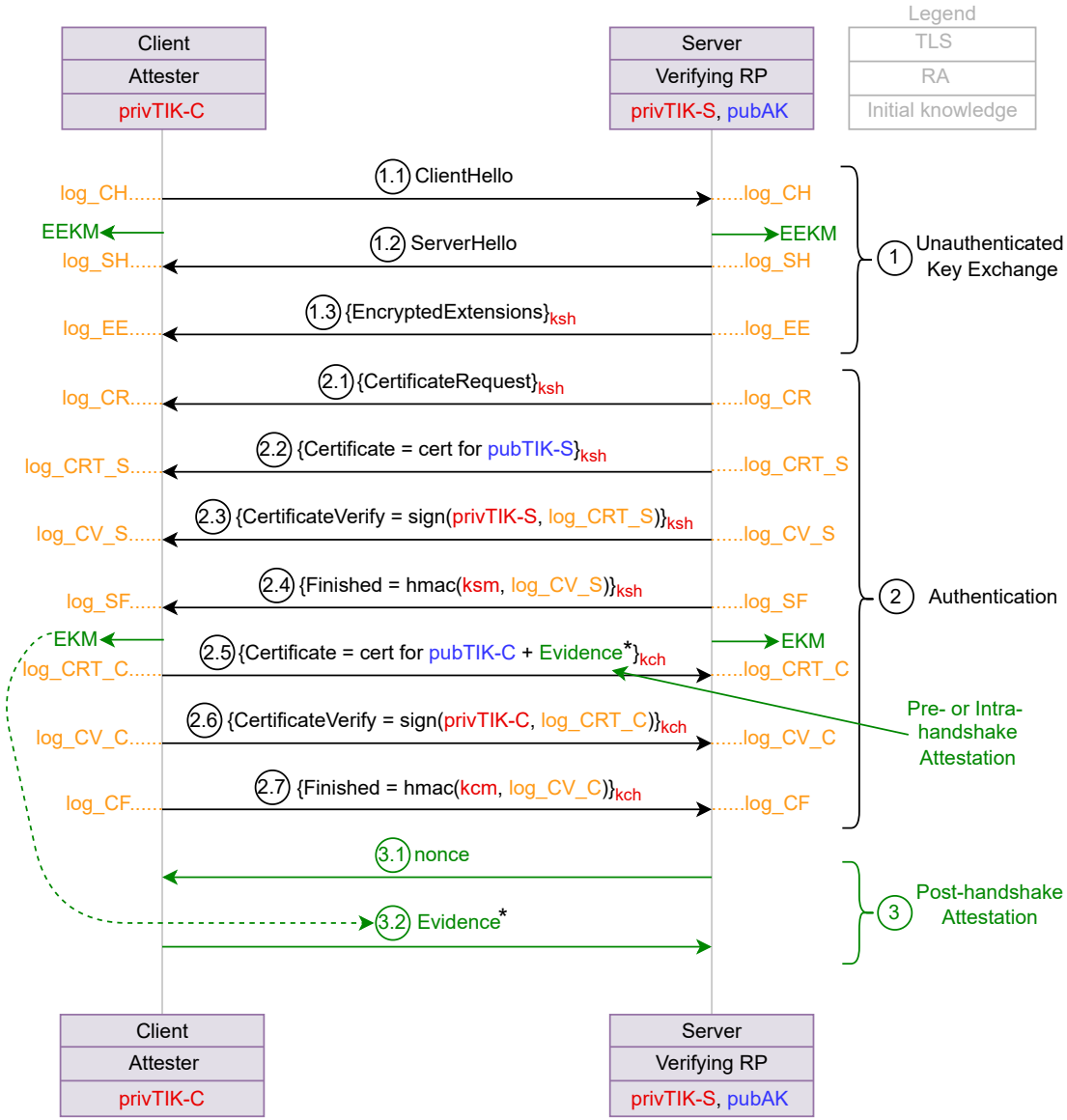
Attested TLS

- TLS 1.3[1]
  - Good for network security
  - Not good for endpoint security
- Use case: Confidential Computing



[1] https://datatracker.ietf.org/doc/html/rfc8446

Generic Protocol (Client as Attester)



What's done: Pre-handshake attestation (Intel's RA-TLS)

- Intel neither specified protocol nor properties
- RATS WG is too vague and incomplete about security considerations
  - RATS Architecture[2], e.g., errata[3]
  - Interaction models[4], e.g., issue[5]
- Tool: ProVerif

Property	Without `privEK` leak	With `privEK` leak
Freshness of evidence	× (1.7 s)	× (6 min 56 s)
Server authentication	✓ (4.6 s)	× (2 min 08 s)

Table: Verification results and times for RA-TLS protocol

[2] `https://datatracker.ietf.org/doc/html/rfc9334`

[3] `https://www.rfc-editor.org/errata_search.php?rfc=9334`

[4] `https://datatracker.ietf.org/doc/draft-ietf-rats-reference-interaction-models/11/`

[5] `https://github.com/ietf-rats-wg/draft-ietf-rats-reference-interaction-models/issues/58`

What we are looking for?

- Seek collaborators knowledgeable in at least one of:
  - TLS
  - Remote attestation
  - Formal methods (Symbolic security analysis)
  - Confidential computing

  and interested in precisely specifying further properties of attested TLS

- Side meetings
  - Basic attested TLS tutorial: Tuesday 9:30-11:30, Wicklow Hall 2A
  - Advanced attested TLS tutorial: Wednesday 9:30-11:30, Wicklow Hall 2A

Pointers to resources

- Pre-handshake attestation[6]
- Intra-handshake attestation[7]
- Post-handshake attestation: Sec. 4 in this paper[8]
- Remote Attestation for Confidential Computing[9]
- Repo for attestation[10]
- Some recent slides and videos[11]
- Slides from side-meeting at IETF 120[12]
- #attested-tls on IETF slack

---

[6] https://www.researchgate.net/publication/385384309_Towards_Validation_of_TLS_13_Formal_Model_and_Vulnerabilities_in_Intel's_RA-TLS_Protocol

[7] https://datatracker.ietf.org/doc/draft-fossati-tls-attestation/

[8] https://www.researchgate.net/publication/367284929_SoK_Attestation_in_Confidential_Computing

[9] https://www.researchgate.net/publication/375592777_Formal_Specification_and_Verification_of_Architecturally-defined_Attestation_Mechanisms_in_Arm_CCA_and_Intel_TDX

[10] https://github.com/CCC-Attestation/formal-spec-TEE

[11] https://github.com/CCC-Attestation/formal-spec-KBS

[12] https://www.researchgate.net/publication/382489639_Presentation_Interactive_Tutorial_Attested_TLS_and_Formalization

Please Applaud!!! (and the crowd goes wild)

ORIGINATOR PROFILE

Invitation to:

Side Meeting on Introduction to Originator Profile Technology

Shigeya Suzuki, Ph.D

Originator Profile Collaborative Innovation Partnership (OP CIP)
(Also: Keio University / WIDE Project)

https://originator-profile.org/en-US/

@ IETF 121 hotRFC, 2024/11/3

What is OP

- Enables end users to identify the originator/publisher of information (content) on the internet, rather than certifying whether content is correct or constitutes mis/disinformation

- What OP provides for the media outlets on the Web
  - Content fragment origin authenticity verification by **Content Attestation**
  - The origin identity — **Originator Profile (OP)** — includes proof of existence, info on multiple third party certification, etc.

OP implementation example on Yomiuri Shimbun Online

Components

- Common Technology (Generic)
  - Identity
  - Data Model
  - Presentation
- Baseline Governance Model

- Application Specific Implementation
  - Web Contents Authenticity

Originator Profile Collaborative Innovation Partnership (OP CIP)

- OP CIP conducts the development and demonstration experiments of OP technology with the participation of major Japanese media including NHK, IT companies, media platforms, advertising companies as part of this project, currently 48 members

- **Members**: Akita Sakigake Shimpo, The Asahi Shimbun Company, WebDINO Japan, ADK Marketing Solutions Inc., The Ehime Shimbun, The Kahoku Shimpo Publishing, Kyodo News, The Kyoto Shimbun, The Kochi Shimbun, The Kobe Shimbun, The Saga Shimbun, SEARCHLIGHT, Sankei Shimbun, The Sanyo Shimbun, Jiji Press, The Shizuoka Shimbun, The Shinano Mainichi Shimbun, The Japan Times, Shogakukan, SmartNews Inc., Dai Nippon Printing, The Chugoku Shimbun, The Chunichi Shimbun, Tokyo Broadcasting System Television, Dentsu Inc., Dentsu Soken, The Niigata Nippo, Nikkei, Nippon Television Network Corporation, Nippon Telegraph and Telephone, Japan Broadcasting Corporation, News Corp, Hakuhodo DY Media Partners Inc., Video Research, The Fukushima Minyu Shimbun, Fuji Television Network, fluct, The Hokkaido Shimbun Press, THE HOKKOKU SHIMBUN, The Mainichi Newspapers, magaport, The Miyazaki Nichi Nichi Shimbun, Momentum, The Yomiuri Shimbun, LY Corporation
- **Individual Members:** Jun Murai (Professor of Keio university, Co-Chairs, Cyber Civilization Research Center), Shigeya Suzuki (Project Professor, Graduate School of Media & Governance, Keio University), Tatsuya Kurosaka (Project Associate Professor, Graduate School of Media & Governance, Keio University),Tatsuhiko Yamamoto (Professor, Keio University Law School)

Participating Companies

For more information:
Public Side Meeting on Monday Lunchtime

- Date/Time: Monday, November 4th 12:30-13:30
- Location: Wicklow Hall 2A

- Intentionally overlap 30min into lunch time
  - 25 min for presentation (with Video), followed by Q&A + Discussions

- Or find and ask me during IETF 121
- Or visit web site:
  - https://originator-profile.org/en-US/
  - FAQ is available: https://originator-profile.org/en-US/faq/

Please Applaud!!! (and the crowd goes wild)

Preventing denial of service attacks on TLS handshakes

Client puzzle and exploration of other approaches

Problem

- TLS handshakes are fundamentally asymmetric in computational effort
- Seems to be actually exploited in practice

source on active attacks: https://www.youtube.com/watch?v=pBNMWvfL05g

Client puzzles

- Direct throttling of client request by requiring them to do calculations
- Nygren draft: https://datatracker.ietf.org/doc/html/draft-nygren-tls-client-puzzles-02
- Revival: https://github.com/tweedegolf/draft-TLS-client-puzzles

(submitted as I-D under draft-venhoek-tls-client-puzzles-00)

Alternate solutions

- Faster signatures (batching)
- Optimizing handshakes/packet handling
- Other suggestions?

Please Applaud!!! (and the crowd goes wild)

TCP_REPLENISH_TIME

HotRFC, IETF 121 Dublin, November 2024

Stuart Cheshire, Apple

Source-Device Bufferbloat

April 2011

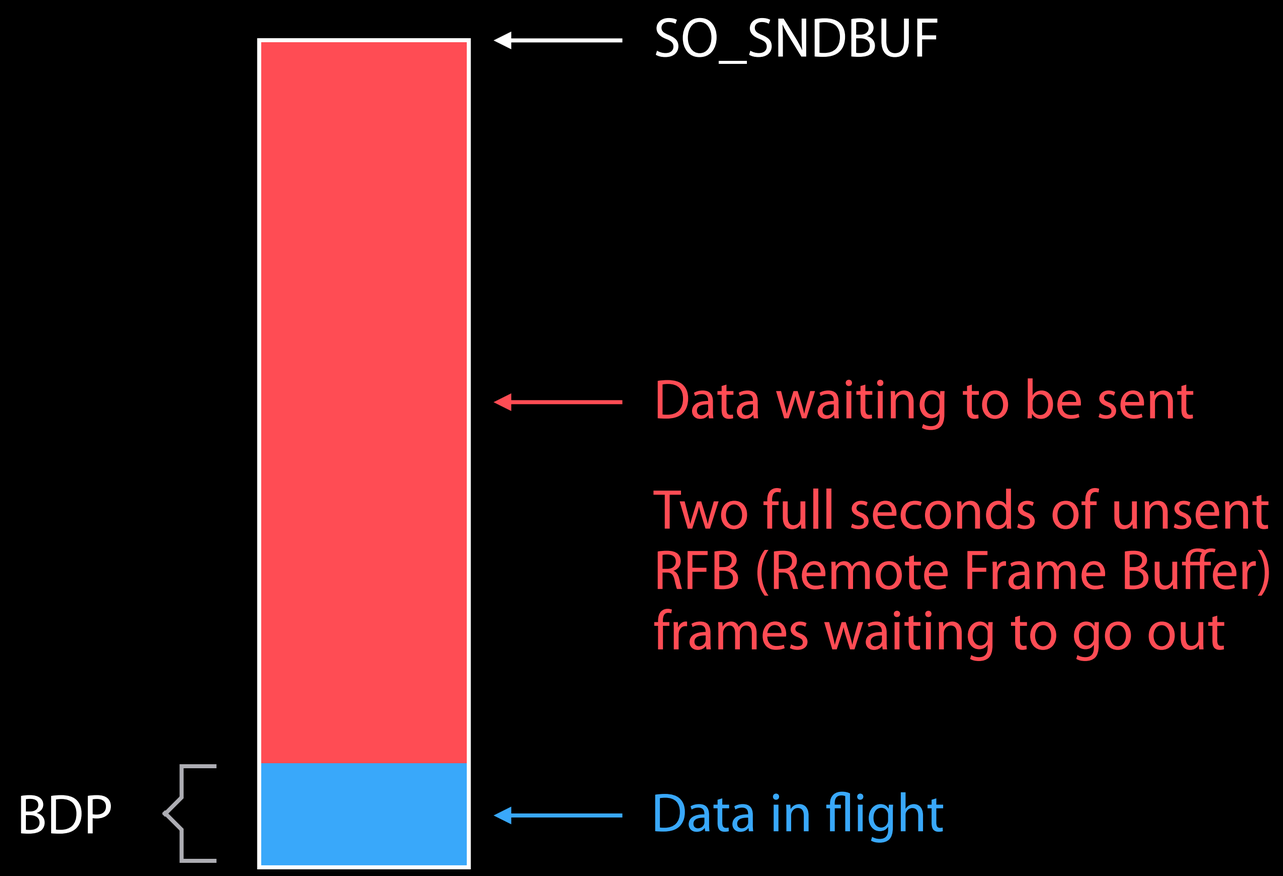
Mac OS Screen Sharing sluggish on slow networks

Network Bufferbloat suspected

Real cause was excessive buffering by the sender

Sluggish Screen Sharing

Source-device Bufferbloat



TCP_NOTSENT_LOWAT

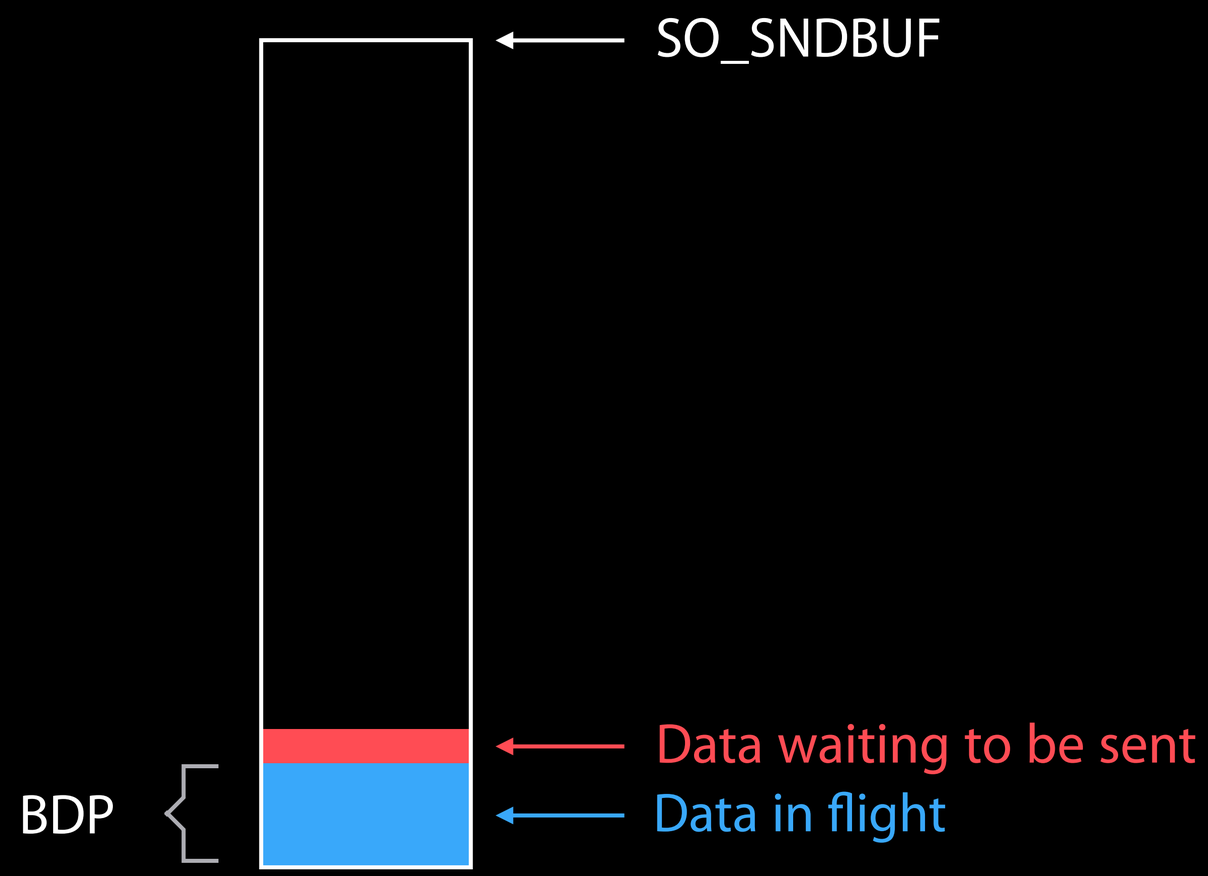
TCP Not-Sent Low-Water Mark

kevent() doesn’t signal application to generate a new compressed frame
until TCP is almost ready to need more data

Fixes excessive sender-side buffering for real-time delay-sensitive applications

See Apple WWDC 2015 video “Your App and Next Generation Networks”

Snappy Screen Sharing
Using TCP_NOTSENT_LOWAT



TCP_NOTSENT_LOWAT problems

Low-Water Mark specified in bytes

16 kilobytes (about ten Ethernet frames) works pretty well, but…

- Can be too much on low-rate networks (e.g., 250 kb/s and less)
- Can be too little on high-rate networks (e.g., Gb/s and above)
- Would be better if specified in time (milliseconds, or microseconds) indicating how much notice the application needs to generate next chunk of data

TCP_NOTSENT_LOWAT problems

Inconsistent across different platforms

On Mac OS and iOS, socket option determines low-water mark

- When unsent backlog falls below low-water mark, application is *signaled* (e.g., via kqueue) to generate more data
- Application can then atomically write as much as makes sense for that application, up to SO_SNDBUF

On Linux, socket option determines high-water mark

- Application is *prevented* from writing more than high-water mark
- Can severely reduce throughput if TCP_NOTSENT_LOWAT set to 16 kB

TCP_REPLENISH_TIME

Opportunity to fix this

New mechanism specified in terms of how much *time* an application needs to generate its next chunk of real-time delay-sensitive data

Make it work the same for all transport protocols, on all platforms

- TCP, QUIC, etc.
- Linux, FreeBSD, Windows, MacOS, iOS, etc.

Side Meeting, 19:00-20:00 Thursday 7th November, Wicklow Meeting Room 4

- If interested, email Stuart Cheshire <cheshire@apple.com> with TCP_REPLENISH_TIME in subject line by noon on Thursday 7th November

May look to form IETF Working Group if people feel that is appropriate next step

Please Applaud!!! (and the crowd goes wild)

Proposal for a new RG

SUSTAIN
Sustainability and the Internet

Ali Rezaki, Eve Schooler, Michael Welzl

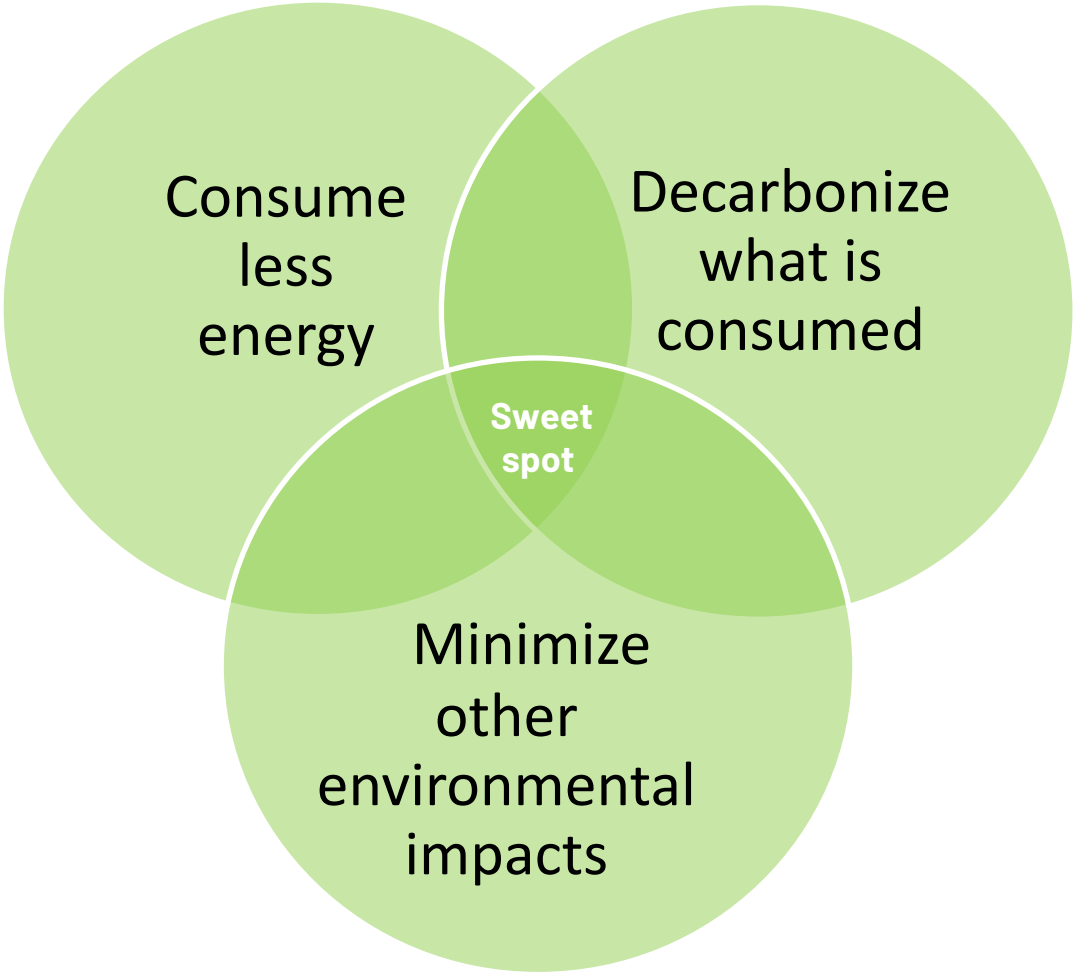
HotRFC @ IETF 121 – Dublin

Sunday, Nov 3rd, 2024

Backdrop

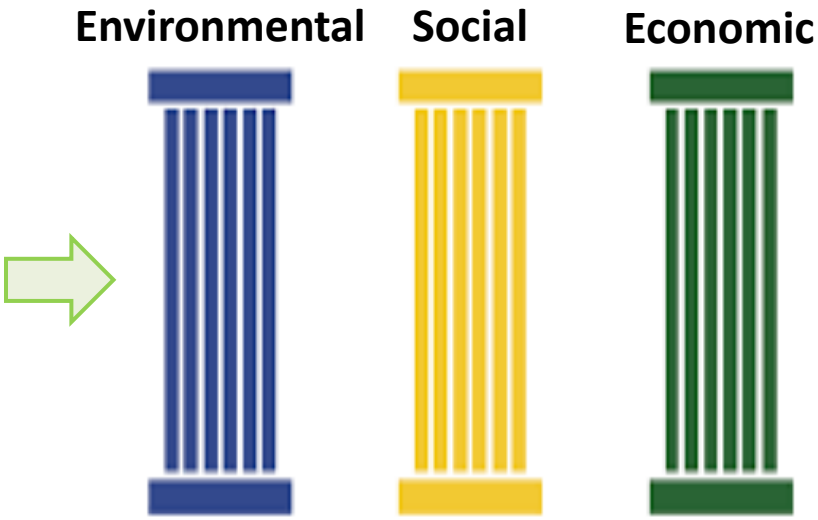
- Urgency to address UN IPCC recommendations
  - 1.5C degree threshold - minimize climate change impact
- Timeline to reduce GHG emissions
  - 50 % by 2030
  - 100 % by 2050
- ICT contribution to GHG emissions sizeable and growing
  - Network impact rivals Data Center
- Exacerbated by growth of AI

Traditional Sustainability Goals?



Broader Sustainability Pillars

"Meet the needs of the present without compromising the ability of future generations to meet their own needs."



SUSTAINABLE DEVELOPMENT GOALS

Vision

Contribute to the advancement of the Internet as a fundamental part of a sustainable and resilient society and planet, through conceptual and evidence-based research collaboration

Scope: From a **Networking Design Perspective…**

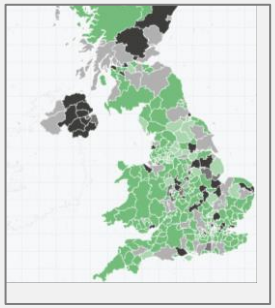
- Explore research challenges developing and operating a sustainable Internet
  - examine **longer-term research**
  - and its **trustworthy dissemination**
- Investigate **architectural and policy implications**
  - without going into advocacy actions
- Consider **footprint & handprint**, *i.e.,*
  - Sustainability of the Internet
  - Internet for Sustainability

Beyond the Technical

Country-Scale Electricity Usage

- Internet networking is on par with many developed nations

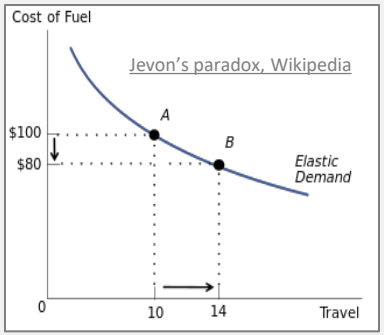
https://carboncopy.eco/local-climate-action



Who/How to effectively, responsibly manage?

Tackling Jevon's Paradox

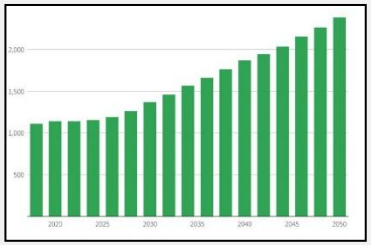
- Increased efficiency → Reduced cost → Greater usage



How to make efficiency gains stick?

Huge eGrid Growth & Transition

- 2x-4x electricity needed to electrify transportation
- Edge-ification and Renewables
- ICT as a virtual battery



Disruption = Opportunity!

More Internet Sustainability Concerns

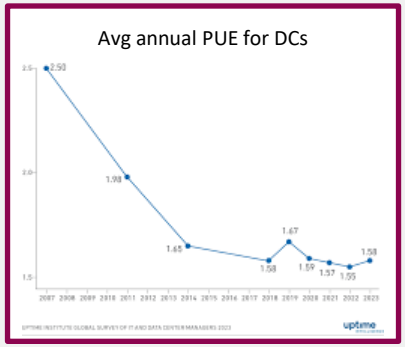
Financial Incentive: Tax Credits

- A huge lever to incent the (US) infrastructure to transition to renewables

Accelerate the uptake of renewable energy!

Policy: DC Standards

- Server power efficiency timelines
- Unintended consequences



Voluntary → Mandated

Ethics

- ***"If country X wants to be a world leader in AI"***
  - **Q:** should they support AI's unbounded use of electricity?
- ***"If AI holds the promise to accelerate innovation"***
  - **Q:** should AI receive special compensation re emissions goals?

Solicit Research Contributions

Investigation

- **Footprint reductions** of Internet networking (environmental, social, financial), with awareness of lifecycles and supply chains
- Environmental **limits & boundaries**, e.g., for safety
- Relationship between **sustainability and architecture,** differing approaches to network design, tradeoffs
- Novel steps toward energy efficiency, energy savings and **energy proportionality**; progress towards overall GHG emissions reductions, like **carbon-aware** routing, carbon-aware traffic steering and carbon-aware data transmission
- The **interplay between energy-networking infrastructures**, *e.g.,* role of renewables to power Internet and on-demand Internet to consume excess renewables

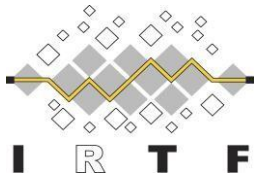
Understanding

- Role of **policy and regulation**
- Potential for **rebound effects**
- **Incentivization** of sustainability
- New methodologies, architectures and strategies to ensure Internet **resilience**

Mode of Operation

- Invite participation from industry, academia, govt
  - Meet regularly, encouraging hybrid participation
- Coordinate with others
  - RGs (ICN, DIN, GAIA, HRPC)
  - WGs (GREEN, TVR, OPSWG)
  - E-impact, ISOC, other SDOs, consortia
- Produce Informational RFCs on SoTA, gaps, etc
  - Defer standardization to the IETF

Come to the Side Meeting!



- **What:** Discuss proposed SUSTAIN RG charter
- **When:** Weds, Nov 6th, 2024 @ 14:30 (UTC+0)
- **Where:** Wicklow Hall 2A

- **Who:**
  Ali Rezaki <ali.rezaki@nokia.com>
  Eve Schooler <eve.schooler@gmail.com>
  Michael Welzl michawe@ifi.uio.no

- **GitHub repository:**
  https://github.com/rezaki-ali/IRTF_SUSTAIN_RG

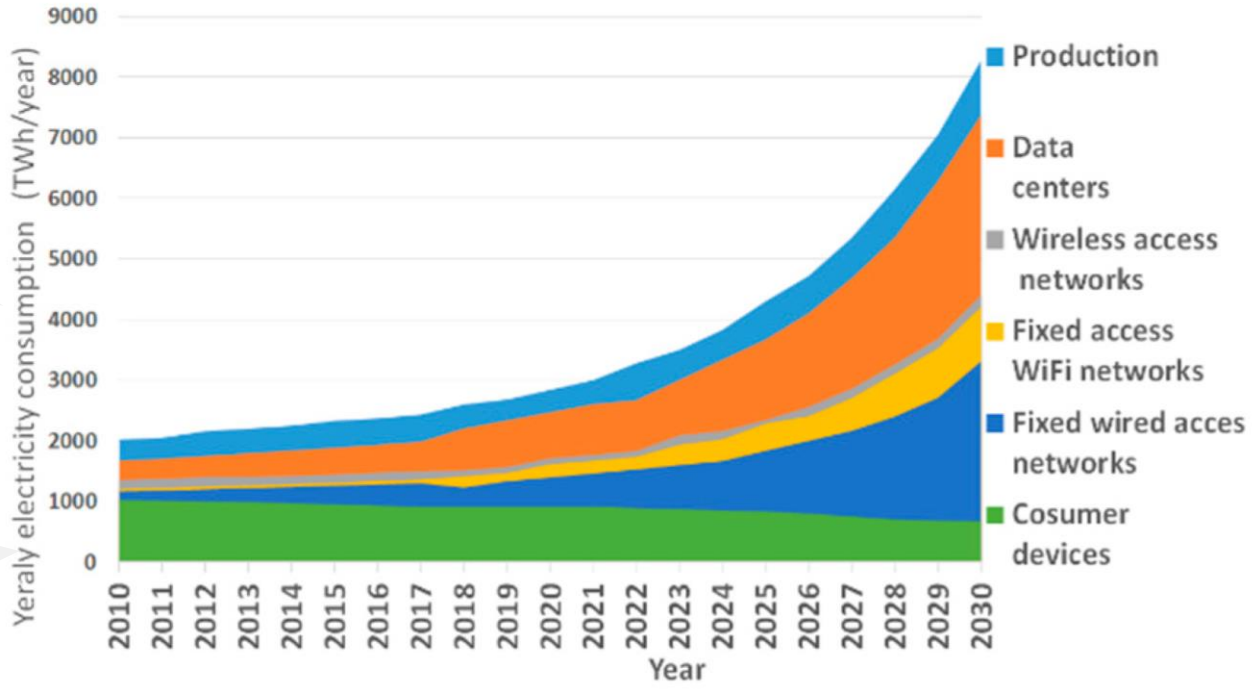
BACKUP

ICT Electricity Usage…**Growing Significantly**

Q: Measured vs Projected?

US consumes ~4000 TWh/yr

UK consumes ~325 TWh/yr



Information Communication Technology (ICT)

projected energy usage as a percentage of total electricity **is notable!**

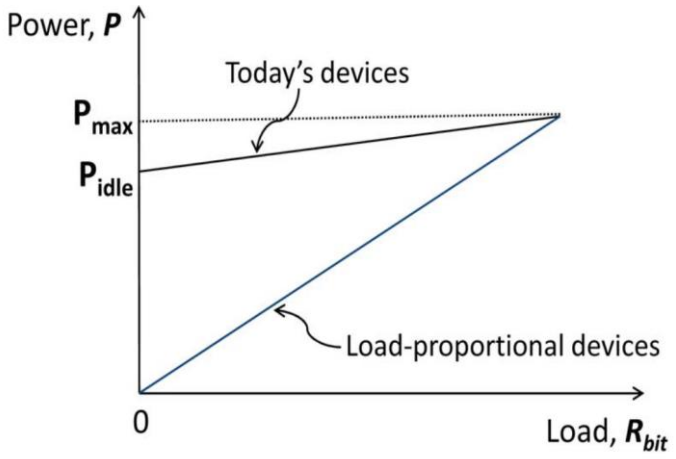
(2%-24% forecasts)

Source: Lorincz, Josip, Antonio Capone, and Jinsong Wu. "Greener, energy-efficient and sustainable networks: state-of-the-art and new trends" Sensors, (2019): 4864.

Sustainable Network Challenges

- **Many Networks are NOT *power-proportional***
  - Same energy expended irrespective of traffic load
- **Network *idle power* is significant**
  - Often very close to max power
- **Networks are vastly *overprovisioned***
  - Few network elements support *sleep states*
- **Networks are not *carbon-aware***

Power Consumption Profile



Source: "Modeling Energy Consumption in High-Capacity Routers and Switches", A. Vishwanath et al, IEEE JSAC, Vol.32, No.8, Aug 2014

Please Applaud!!! (and the crowd goes wild)

UNIVERSITY OF
OXFORD

DEPARTMENT OF
ENGINEERING
SCIENCE

Real-Time Telemetry for Carbon-Aware Networking: Measuring and Reducing Environmental Impact

Presenter: Dr Omid Tavallaie
Postdoctoral Researcher
University of Oxford

IETF 121 Dublin
November 2024

Growing Environmental Impact of Networking

- The Information and Communications Technology (ICT) sector, which includes data networks, currently consumes approximately 2-3% of the world's electricity.
- By 2030, this could grow to 8-21% if left unchecked due to rapid global internet expansion and increased device usage.
- Unlike data centers, which have seen improvements in efficiency, networks have lagged behind
  - complexities in measurement
- Data transmission has become a significant, yet often overlooked, source of carbon emissions.

Challenges in Measuring Network Power Consumption

- Quantifying and subsequently reducing the consumption of electricity is no easy task:
  - Many contributors (client device, infrastructure, communication links)
  - Lack of awareness of the problem
  - Lack of standards
  - Lack of tools for collecting data

- Current network monitoring tools collect traditional metrics (latency, throughput, and packet loss).
  - Related to performance or security, rather than power consumption and its link to carbon impact

- Much of the work on power consumption has focused on data centers, rather than end-to-end networked systems.

Carbon Intensity as a Key to Network Emissions

- Knowing the total electricity usage is not enough.
- The carbon-intensity of that electricity must be derived to determine the carbon footprint of network elements.
- Carbon intensity is defined as the amount of carbon by weight emitted per unit of energy consumed.
- The data that we do have suggests that networks are a dominant component in the carbon footprint of digital infrastructure.

Enabling Real-Time Carbon Efficiency in Networking

- To properly account for the carbon efficiency of networking, we argue for an end-to-end approach, specifically:
  - Devices should be able to report their real-time or near real-time electricity consumption.
  - Devices should be able to report the carbon-intensity or quality of consumed electricity.
  - Applications and services should react in (near) real-time to carbon-related information collected from the network.

Challenges in Network Telemetry for Carbon Reporting

- Network equipment manufacturers tend to report the maximum power consumption of a platform.
  - The difference between average and maximum may be large (or small).
  - This may not accurately represent the actual platform carbon emissions.

- The absence of hardware support within the platform does not mean that we need to wait for new devices to come to the market.
  - It is possible to leverage proxy data that will indicate usage.

- To make use of the real-time information, there is a need for an end-to-end reporting mechanism.
  - Similar to in-network telemetry used for end-to-end network performance

Challenges in Network Telemetry for Carbon Reporting

- Electricity consumption is not an indication of carbon emissions.
  - The carbon intensity of the energy source must be factored in.

- A distinction could be made between elements consuming electricity from renewable energy sources versus fossil fuel.

- The availability of carbon intensity data is not without its challenges:
  - While many regions globally are making carbon intensity data available publicly, coverage is incomplete.
  - The frequency of the data updates varies considerably across regions.
  - The measurement data must also be verifiable.

Challenges in Network Telemetry for Carbon Reporting

- Both the energy provider, and the network operator, would need to add new support.
- The energy provider should send electricity-quality information (periodically or through dedicated API).
- The network operator should process and propagate this information as part of in-network telemetry (INT) updates.

Conclusion

- Networking needs to be carbon-efficient, like any other part of digital infrastructure.

- To achieve real progress, standard metrics need to be supported and reported by network devices.

- We call on the IETF community to join the effort to define these metrics. Together, we can make networking truly green.

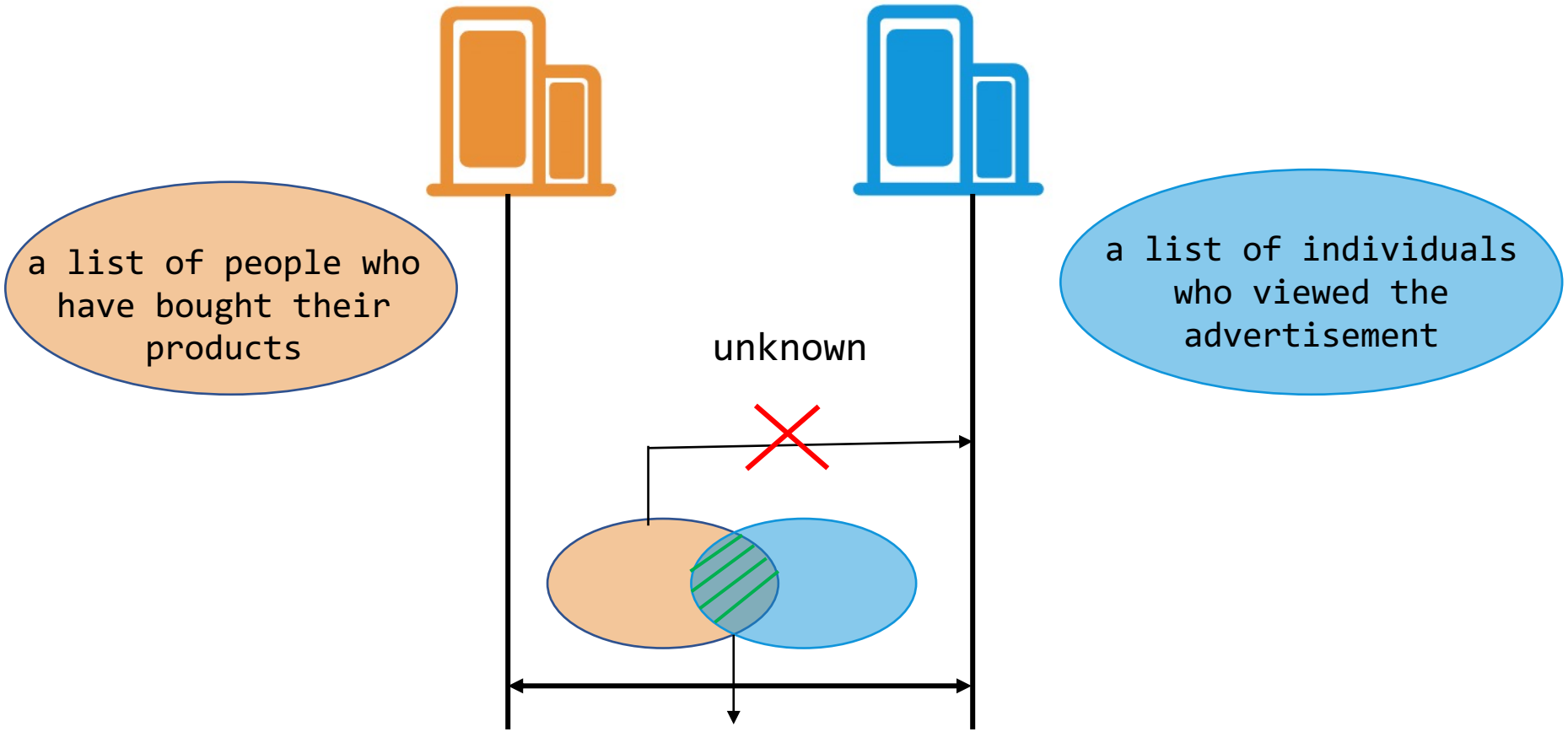
Please Applaud!!! (and the crowd goes wild)

PSI based on ECDH

Presenter: Wenting Chang from Alipay

Use case 1: Joint marketing

Company A and Company B have their own customer lists and want to work together on a joint marketing campaign to target customers who may be interested in both companies. Using PSI technology, two companies can identify the intersecting customer base.



Using ECDH-PSI, the effect of an advertisement can be accurately calculated, without revealing any extra information about the users.

Use case 2: Promotion of bank card user activation

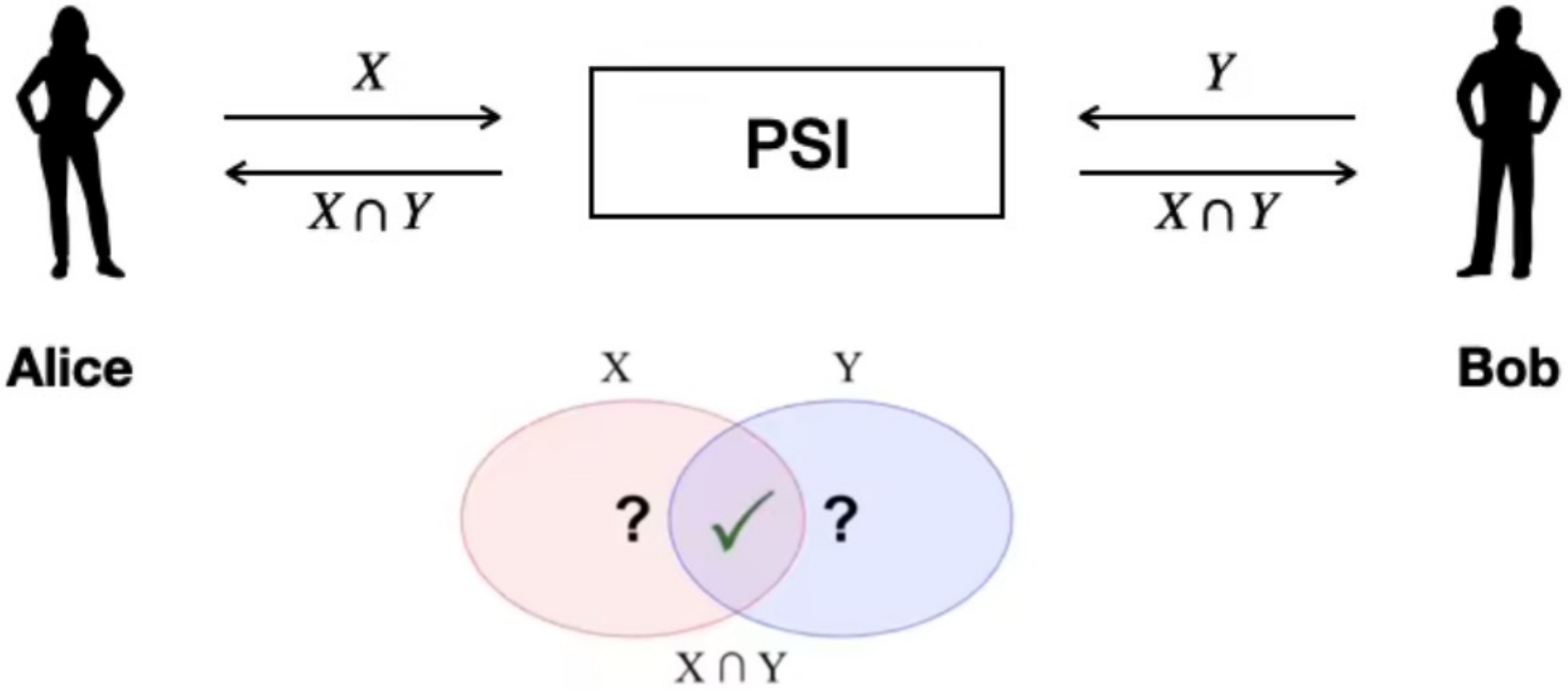
Banks implement various initiatives to attract new users to open bank cards and make their first transactions. For inactive bank card users, banks will focus on popular payment scenarios such as grocery and dining expenditures, offering payment discounts to encourage users to transition to bank cards for transactions.

Reach out online shopping customers to use bank card

offer discounts to encourage users to pay money with bank card

Banks perform PSI with e-commerce and other platforms to identify potential targets for user activation.

Private Set Intersection (PSI) enables between two or more parties to **identify overlapping data elements while preserving the confidentiality of each party's complete dataset.**



- **A protocol** to negotiate required parameters and exchange data
- The negotiation and data **message structure** to realize grammar and semantic consistency

PSI algorithm comparison

PSI algorithm	Characteristic
HASH-based PSI	• higher performance • lower security, e.g. unilateral exhaustive attack
Elliptic Curve Diffie-Hellman (ECDH) based PSI	• limited communication bandwidth • moderate computation requirement • be capable for handling data at the scale of billions
Garbled Circuit based PSI	• higher communication bandwidth • higher computation requirement • Higher design complexity
oblivious transfer (OT) based PSI [1)]	• higher communication bandwidth • lower computation requirement
Vole based PSI [2)]	• algorithm is continuously iterative • lower communication bandwidth • easily construct malicious security PSI
Fully Homomorphic Encryption based PSI [3)]	• higher computation requirement • lower communication bandwidth • fully homomorphic algorithm is still evolving

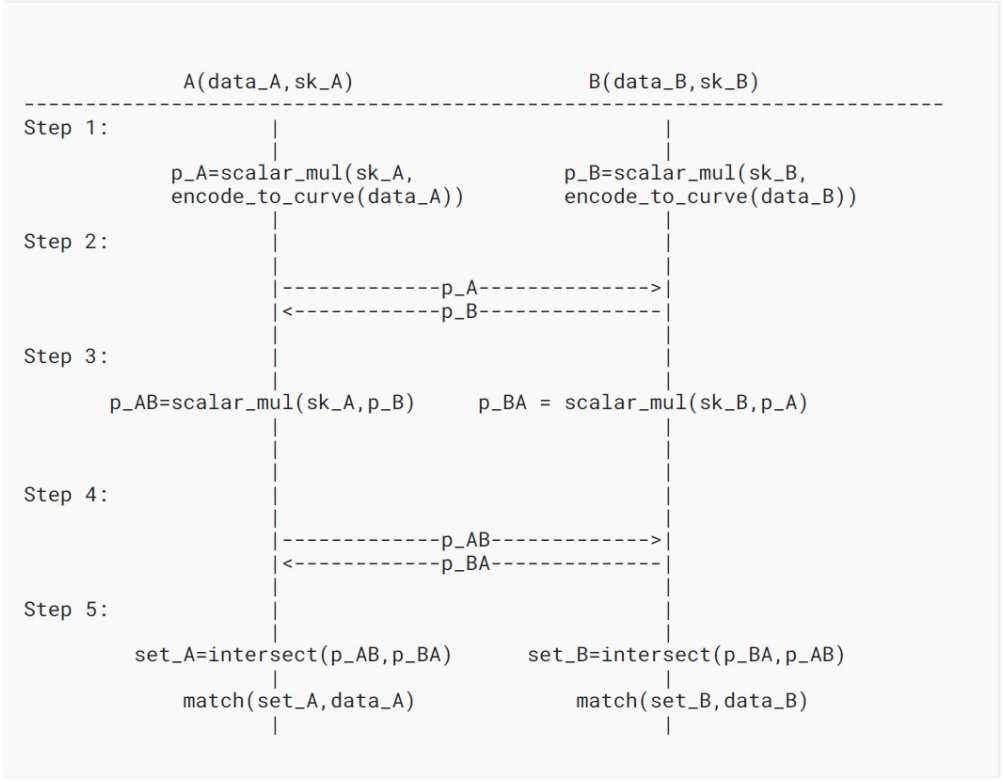
This contribution focus on ECDH-PSI algorithm, since it's readily deployable with limited bandwidth demands and strong security, and the performance can be improved by multithreading and distributed optimization

1) Vladimir Kolesnikov, Ranjit Kumaresan, Mike Rosulek, Ni Trieu. Efficient Batched Oblivious PRF with Applications to Private Set Intersection
2) S.Raghuraman, P. Rindal. Blazing Fast PSI from Improved OKVS and Subfield VOLE
3) Hao Chen, Zhicong Huang, Kim Laine, Peter Rindal. Labeled PSI from Fully Homomorphic Encryption with Malicious Security,

Overview of ECDH-PSI algorithm

In ECDH-PSI, both participants agree on a Elliptic Curve group parameter `G` and generate ECDH key pairs over `G`. The keys are then used to mask the original data with scalar multiplications.

- Step1: A participant maps its data items to points over an elliptic curve with `encode_to_curve`, and mask the points locally with its own private key by `scalar_mul`.
- Step2: A and B exchange their locally masked data as EC points.
- Step3: Upon receiving the masked data from its partner, a participant doubly masked the received points with its private key.
- Step4: A participant sends the doubly-masked points back to its partner.
- Step5: The participant calculates intersection of the set calculated in Step 3 and the set received in Step 4, and finally outputs the original data corresponding to the intersection.



Overview of ECDH-PSI

- **Proposal:** https://datatracker.ietf.org/doc/draft-ecdh-psi/
- **Code:** https://github.com/secretflow/interconnection

Thanks!

Q&A

Contact: wenting.chang@antgroup.com

tianwu.wyc@antgroup.com

Please Applaud!!! (and the crowd goes wild)


See you at
IETF 121!