Sidecar: Secure and Efficient Out-of-band Call Metadata Transmission

David Adei, Varun Madathil*, Nithin Shyam S., and *Bradley Reaves*

North Carolina State University, *Yale University

NC STATE UNIVERSITY

Yale

Views from the Ivory Tower

Our Goals

- Learn more about your needs
- Share ideas, not demands
- Show prototypes, not finished products or standards

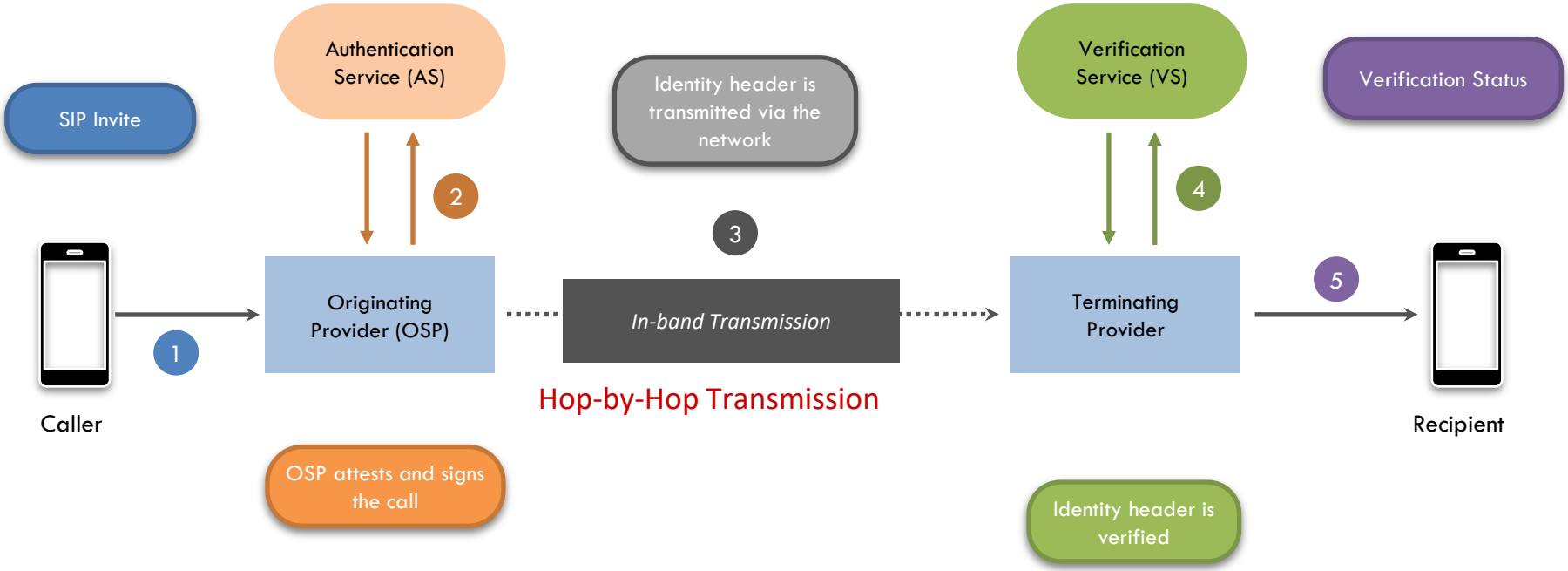
Preprint: https://go.ncsu.edu/sidecar

STIR/SHAKEN is just the beginning

- What properties and features should we consider?
  We've already talked about branded calling, called party authentication, mutual authentication, number intelligence, end-to-end, digital identity…

- How do we make the next systems easier to deploy and interoperate?
  STIR/SHAKEN was a big undertaking. How many more of these do we want?

STIR/SHAKEN Architecture



Challenges Inherent in Hop-by-Hop Transmission

- Still need universal adoption for every new development
  We now have STIR/SHAKEN, but what about RCD? And the next thing?

- This is still a problem even in an all-IP network!
  Still no guarantee that TSPs will get the data.

What if we had done Out-of-Band instead?

- Out-of-band means only OSP and TSP need to support new things
  Early adopters get benefits immediately!

- But we now worry about the OoB infrastructure!
  Is it open and accessible? And if so, how can it be secure?

Challenges of Out-of-Band

- Every Call Placement Service (etc.) is a Point of Compromise
  The infrastructure you run is secure, but what about your competitors?

- "Compromise" means "data breach" or "CPNI violation"
  Nation-state espionage, call history harvesting, peering relationship information

- Who should get to submit/retrieve data for a call?
  How can the infrastructure control access to this sensitive data?

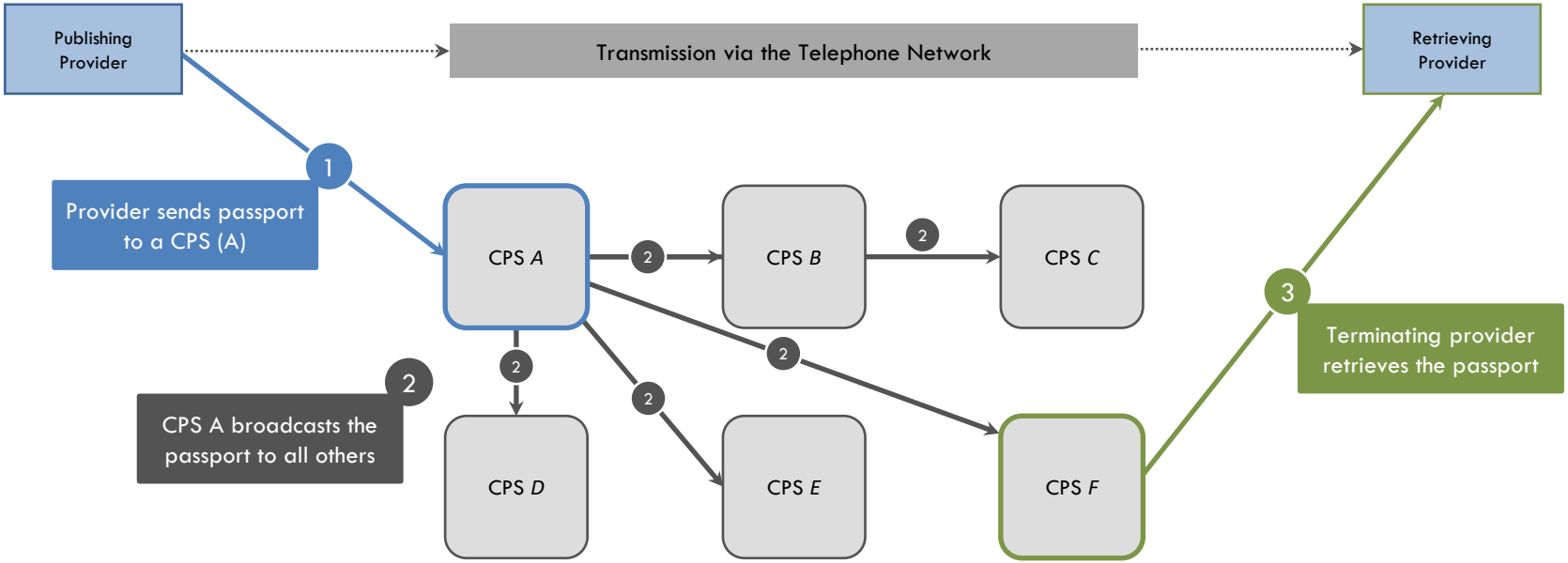
- New infrastructure dependencies
  What do you do if your OOB provider or peer goes down?

Sidecar is Out-of-Band *without the Baggage*

- Can carry arbitrary data – not tied to STIR/SHAKEN
  Supports advanced authentication/extensions to STIR/SHAKEN and real-time multimedia sharing
- All data sent OoB is opaque. Impossible to learn any call details from OoB.
  All your customer data and commercial arrangements are secret
- Cryptographically Enforced Record Expiration
  Records unrecoverable after specified retention period
- Resilient Network Architecture with *Tunable Decentralization*
  Sidecar is designed to allow CPS machines to come and go easily.
  No single points of failure
- Fewer resources, higher availability, equivalent call setup time
  Compared to ATIS 1000096: SHAKEN Out-of-Band PASSporT Transmission Involving TDM Networks

How does Sidecar work?

Let's start with OOB-S/S (ATIS 1000096)



Objectives

- Confidentiality for both Subscribers and Providers
  Protect subscribers' privacy provider traffic patterns from all parties not directly responsible for routing the call.

- Resilient and Efficient Network Architecture
  Network should handle CPS joining and leaving, distribute load equally and resilience to compromise

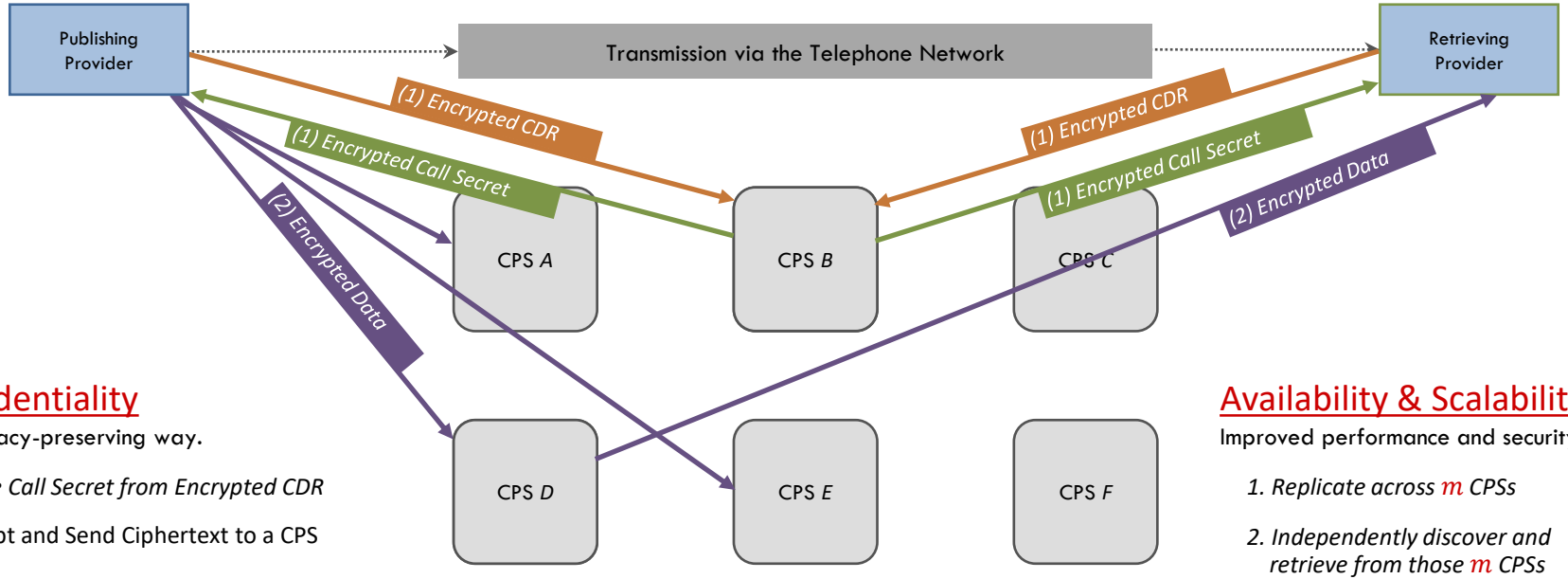
Three Neat Tricks

- Detailed CDRs are only available on-path
  If you know fine details about the call, you're carrying it.

- Oblivious Pseudo-Random Function (OPRF)
  Alice can encrypt data for me without reading the data!

- Content Addressing Distributed Hash Tables
  Originally used in P2P systems like KaZaa and BitTorrent
  Splits data across a bunch of participants who can come and go

Sidecar Oversimplified



Confidentiality

In a privacy-preserving way.

1. *Derive Call Secret from Encrypted CDR*
2. Encrypt and Send Ciphertext to a CPS

Availability & Scalability

Improved performance and security

1. *Replicate across m CPSs*
2. *Independently discover and retrieve from those m CPSs*

Correctness & Security Issues Resolved

- Content Addressing and Load Balancing
  Independent, Uniform and Consistent CPS discovery (Offline/Local) as a function of the CDR

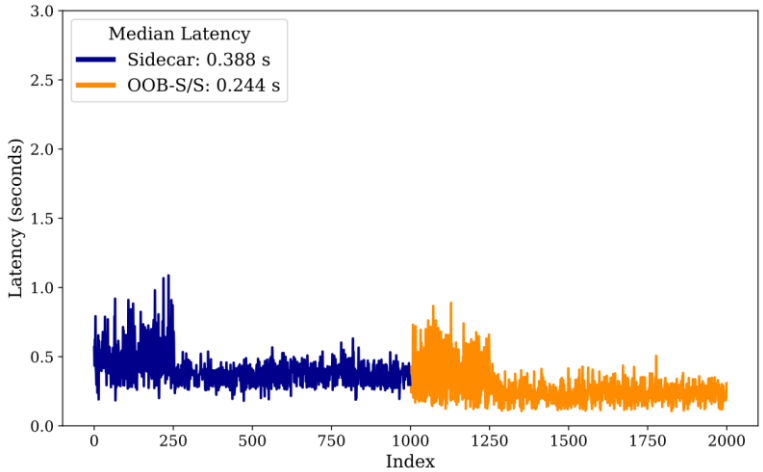
- Key Server Security and Resilience to Compromise
  Distribute Key Server role across n CPS operators

- Record Expiration Enforcement
  Consistent key rotation sub-protocol among Key Servers.

- Rigorous Security Guarantees
  Provide formal guarantees for security properties Sidecar claim to provide

Results - End to End Call Delay Comparison

Despite the extensive cryptographic guarantees, our approach adds only a fraction of a second to the latency experienced by subscribers placing and receiving calls.



Latency measured in seconds

Preprint: https://go.ncsu.edu/sidecar

Results - Availability

Sidecar gives "six nines" uptime on commodity cloud infrastructure

Just 32 seconds annual downtime using nodes with 99.0% availability

Results - Resource Requirements

Sidecar requires modest compute and bandwidth resources:
just $25 for CPSs and $35 for a provider (1000 calls per second) to support 2 billion daily calls across the US.

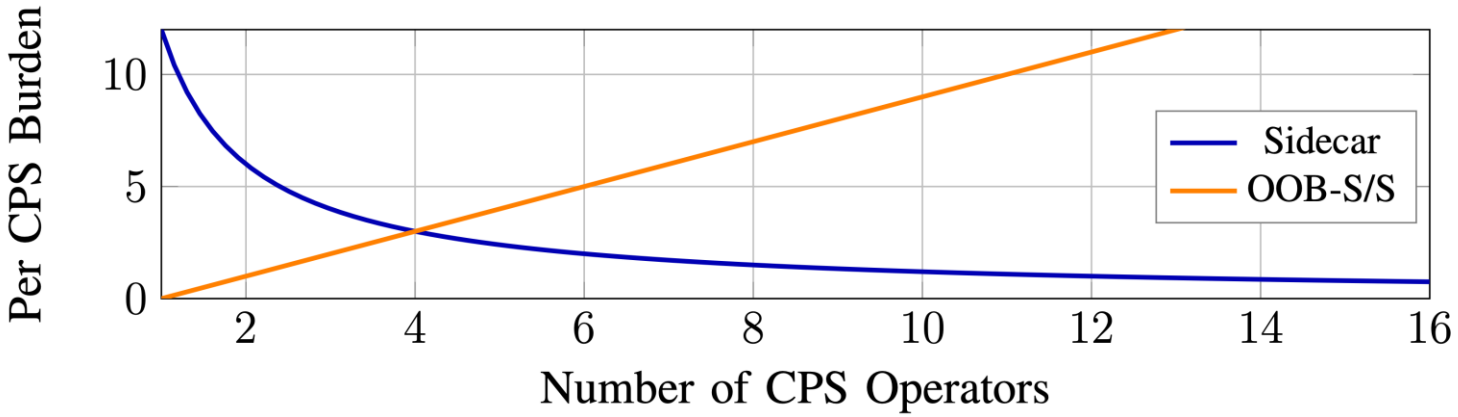
Based on AWS EC2 pricing

Party	vCPUs	Memory	Storage	Bandwidth
CPS—Key Servers	11	7 GB	71 GB	30 Mbps
CPS—Message Stores	10	7GB	71 GB	100 Mbps
Median Provider	29	23 GB	X	360 Mbps

Compute isn't going to be the expensive part

Results - Performance

Adding more CPSs to Sidecar improves both performance and security.



Key Takeaways

- There are more properties that we need for trustworthy telephony than just attestation
- Computer Science has developed techniques that allow us to **mitigate the disadvantages** of a typical OOB approach **while reaping the benefits**
- Academics want to help!

Thank You

David L. Adei: dahmed@ncsu.edu
Brad Reaves: bgreaves@ncsu.edu

Robocall⊛Science
https://robocall.science

Preprint: https://go.ncsu.edu/sidecar