The Powers of eBPF for Telco Networks

David Soldani
SVP Innovation and Advanced Research
Rakuten Mobile

Speech at The 6G series workshop by Hexa-X-II
13 February 2024
https://hexa-x-ii.eu/the-6g-series-workshop-by-hexa-x-ii-feb-2024/

Rakuten

HEXA-X-II

Biography – Dr David Soldani

Top 50 thought leader and influencer in 2023
9,100+ Citations on Google Scholar
26,000+ followers on LinkedIn
500,000+ downloads / 1 year on LinkedIn

WORK EXPERIENCE

~ 25 years active in ICT field, globally

- ***Future wireless, network, Open RAN, cybersecurity, artificial intelligence and cloud-native observability, security and networking technologies***
- *500+ successful projects for 4G, 5G and 6G systems, cloud-native technologies, security controls and assurance, and AI service applications*
- *1000+ quality deliverables (papers, books, standards, proof of concepts, etc.) and 1000+ lectures and public talks*

~ 2 Years: Rakuten

- *2021-Now: Chief Information and Security Officer (CISO), Rakuten Symphony ➔ **SVP Innovation and Advanced Research, Rakuten Mobile Inc.***

~ 10 Years: Huawei Technologies

- *2018-2021: CTO & CSO Huawei, ASIA Pacific Region. (Chairman of **IMDA 5G Task Force**, Singapore.)*
- *2009-2016: Head of Central Research Institute (CRI), VP Strategic Research and Innovation, Europe*

~ 15 Years: Nokia

- *2016-2018: Head of 5G Technology, e2e, global*
- *1997-2009: R&D Director, Finland; and Network Planning Manager, Italy*

~ 2 Years: Italian Military Navy

- *Officer at Italian Institute of Telecommunications and Electronics (MARITELERADAR), Livorno, Italy*

QUALIFICATION

- *2018-now: **Adjunct Professor** **at University of New South Wales (UNSW)**, Faculty of Engineering, Australia*
- *2014-2018: **Industry Professor** at University of Technology Sydney, Australia; **Visiting Professor** at University of Surrey, UK*
- *2002-2006: **Doctor of Science (DSc) in Technology** degree with distinction from Helsinki University of Technology (TKK), Finland*
- *1989-1994: **Laura** in Electronic Engineering (MSc) with magna cum laude from Università degli Studi di Firenze, Italy*

Outline

The path to 6G

The powers of eBPF

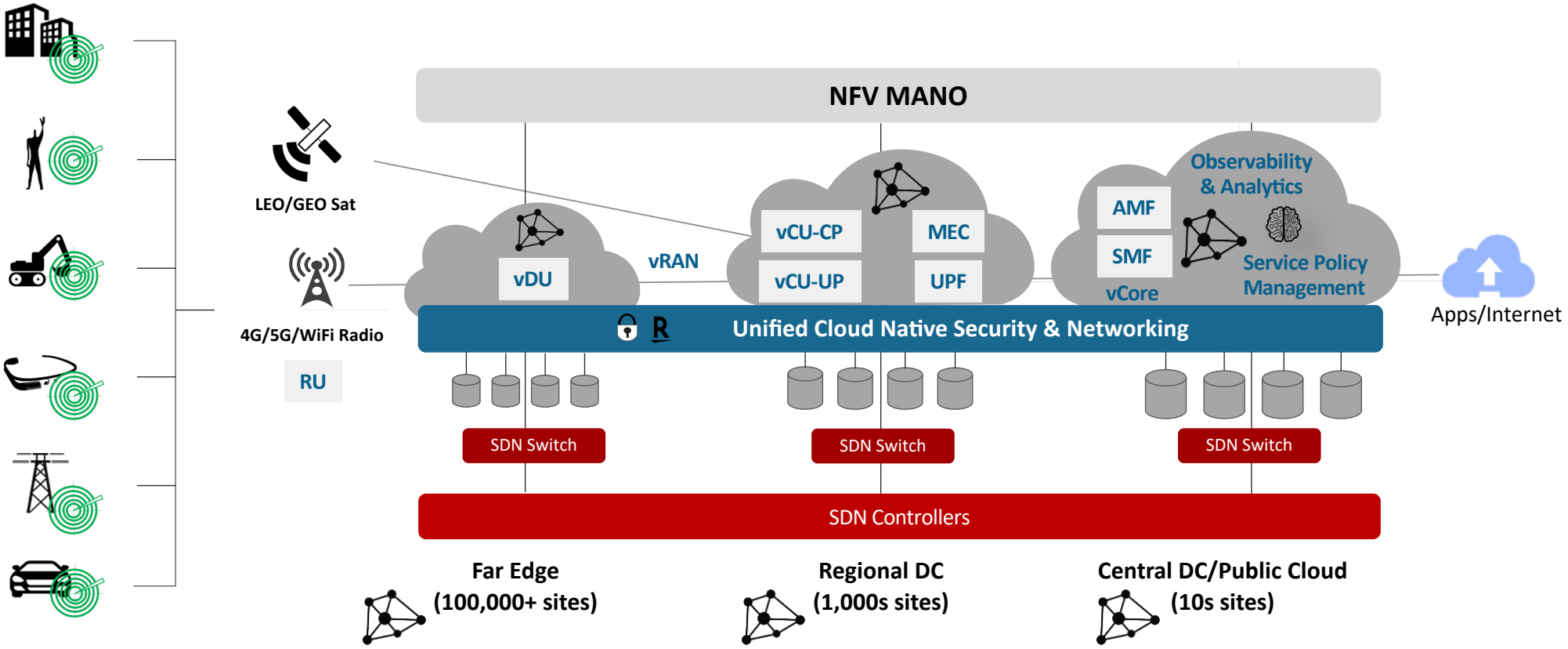
eBPF for Kubernetes

Sauron eBPF platform

Conclusions

Current architecture and design principles – As is today

5G RADIO	HARDWARE	CLOUD INFRA	PLATFORM	OPERATIONS
O-RAN ARCHITECTURE	STANDARD COTS	COTS-BASED MEC DESIGN	CLOUD NATIVE TELCO PLATFORM	AUTOMATION & AI OPS
Disaggregated and Cloud Native RAN Architecture	x86 COTS hardware for the entire network infrastructure	Optimal mix of edge data centers and central data centers	Unified E2E platform designed for elasticity, security, networking, and scalability	Automation for everything supported with AI models



40%

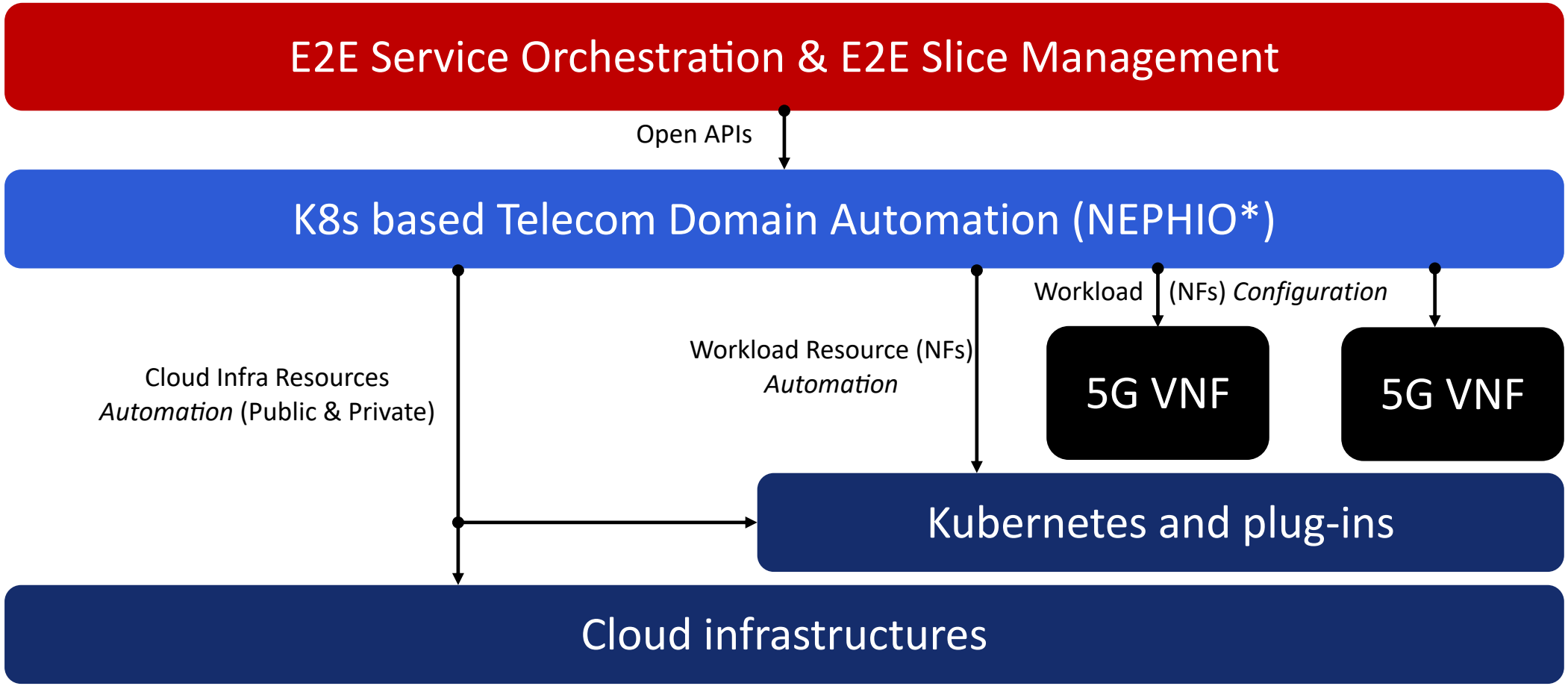
CAPEX reduction

+

30%

OPEX reduction

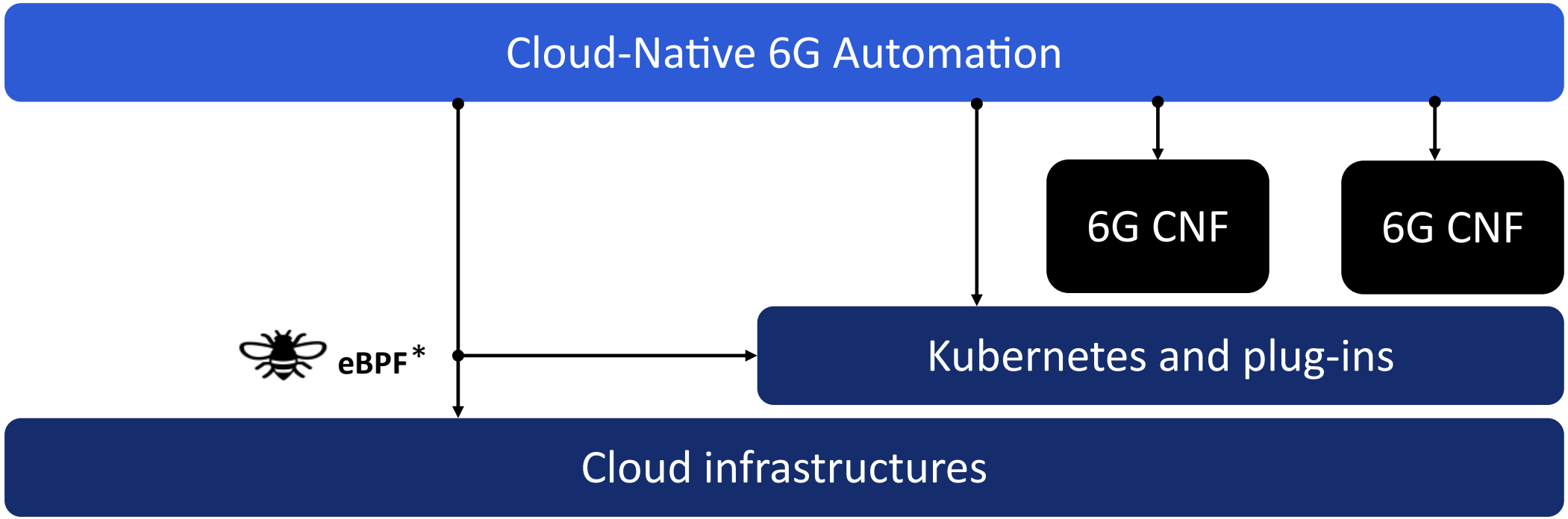
5G reference architecture (from networks-as-devices to networks-as-software) – As is



*) Nephio aims to make Kubernetes the de facto standard for *declarative* (imperative ➔ descriptive) management within telecom, by establishing *common templates* that conform to both Open RAN (O-RAN Alliance) and 3GPP specifications for automation/configuration management.

6G reference architecture: cloud native and secure by design (powered by eBPF) – To be

The extended Berkeley Packet Filter (eBPF) has the potential for **networking** (SDN of cloud native age and bridge cloud), **observability** everywhere and **security assurance** with improved QoE



*) eBPF let you run custom code in the kernel when the kernel or an application passes a certain hook point (system call, function entry/exit, kernel trace point, network event, etc.)

Outline

The path to 6G

The powers of eBPF

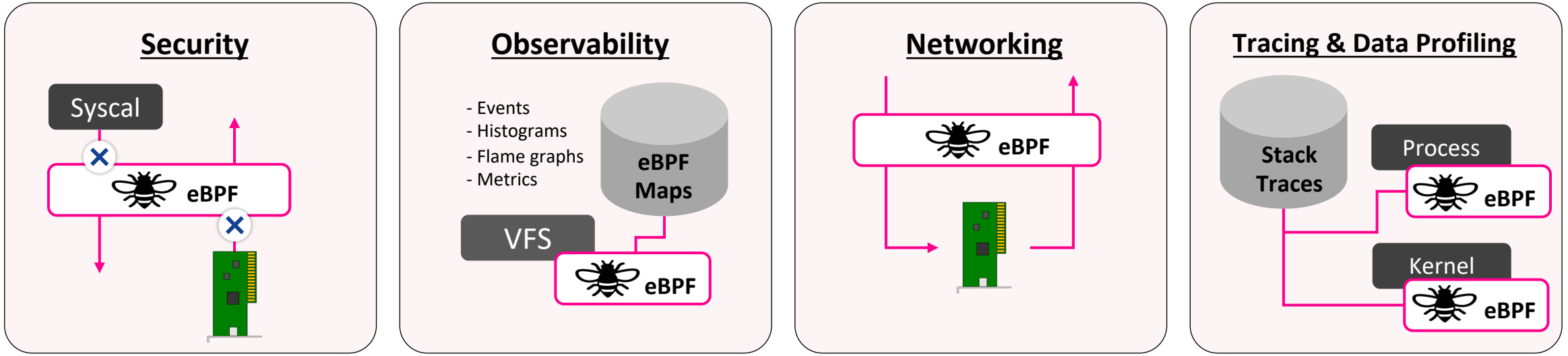
eBPF for Kubernetes

Sauron eBPF platform

Conclusions

What is the extended version of the Berkeley Packet Filter (eBPF)?

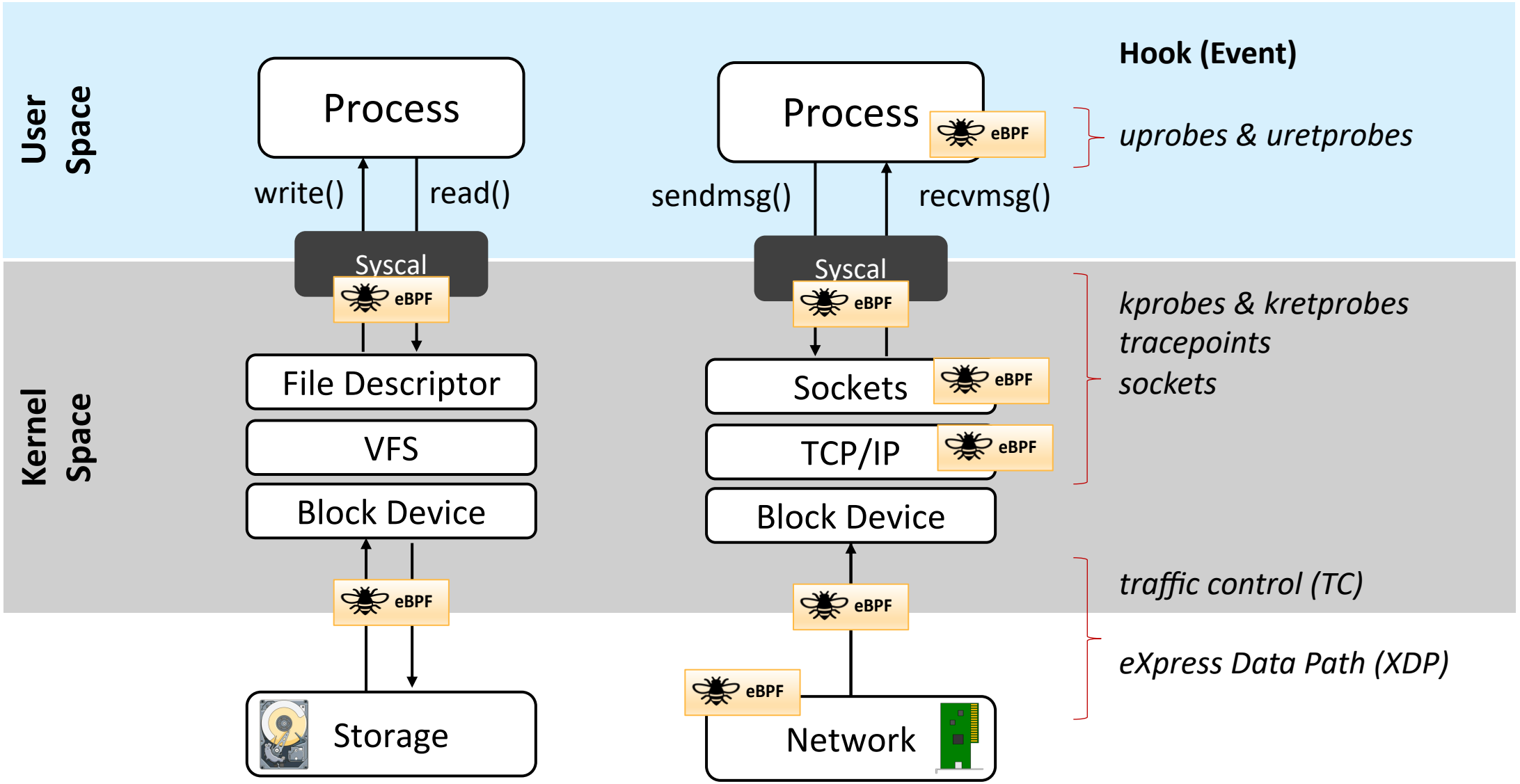
- eBPF is a **general-purpose engine (virtual machine)** to run programs in the Linux kernel (and now Windows) and **instrument** its behavior without changing kernel's **source code** and introducing any **harm** to its stability
- **eBPF programs** are **portable** between kernel versions, **atomically updateable**, avoiding workload disruption and node **reboot**, and **verified** at load time to prevent kernel crashing or other instabilities



SDKs & Packaging: cilium/ebpf · libbpf C++ · libbpf-rs | redbpf | Aya Rust · Bumblebee · BPF Compiler Collection (BCC)

Platform: Since 2014 eBPF Linux Runtime · Now eBPF Windows Runtime

Examples of eBPF program types for Tracing & Networking and attachment types



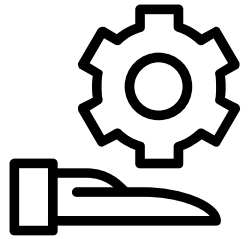
Why eBPF?

Programmability

- eBPF makes the kernel programmable (CO-RE, BTF, and *libbpf*) at **runtime** and ensures the **safety** of the *kernel* and **stability** of loaded *programs*

Visibility, Control and Performance

- **Performance tracing** of pretty much any aspect of a system (one host OS)
- **High-performance** networking (**2.5x** vs. regular Iptables, **4.3x** over IPVS for load balancing, **O(n) to O(1)** operation for looking up a rule in a table*, where *n* is the number of rules)
- **Real-Time threat detection and response**, detecting and (optionally) preventing malicious activity



Overhead

- eBPF low overhead (e.g., ***"sidecar-free" service mesh***, ***XDP offloading – direct path***) makes it ideal for **production** level cloud native environments for **Telco**

"eBPF is to Linux kernel (and now MS Windows) what a Java-script is to Web browser"

*) Updates to iptables aren't the only performance issues: looking up a rule requires a linear search through the table, which is an O(n) operation, growing linearly with the number of rules. Cilium uses eBPF hash table maps to store network policy rules, connection tracking, and load balancer lookup tables, which can replace iptables for kubeproxy. Both looking up an entry in a hash table and inserting a new one are approximately O(1) operations, which means they scale much, much better.

Outline

The path to 6G

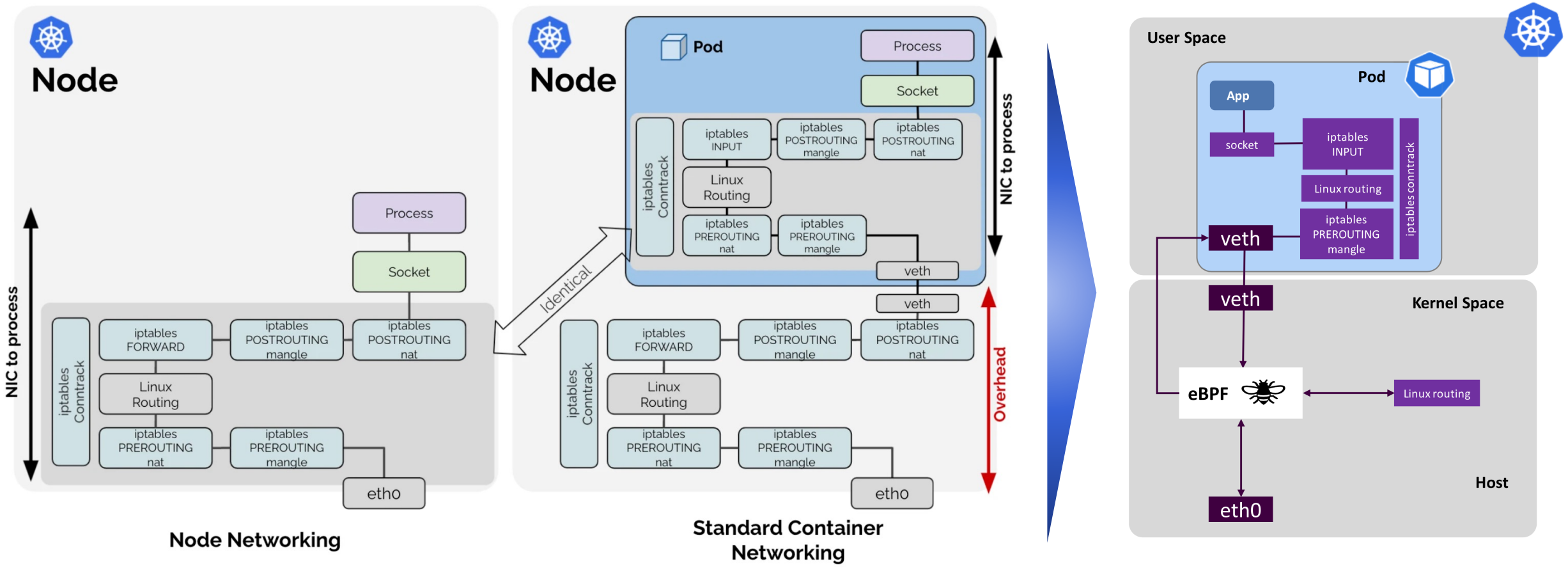
The powers of eBPF

eBPF for Kubernetes

Sauron eBPF platform

Conclusions

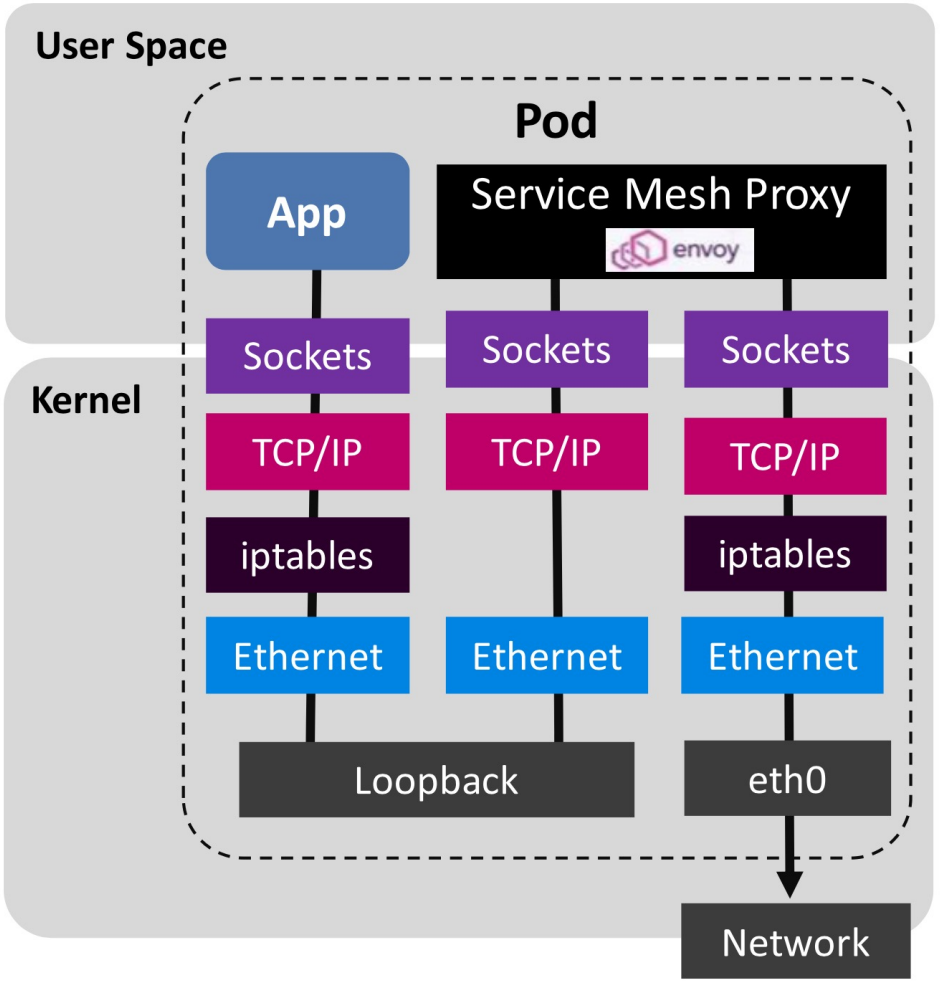
How eBPF advantages for pod networking



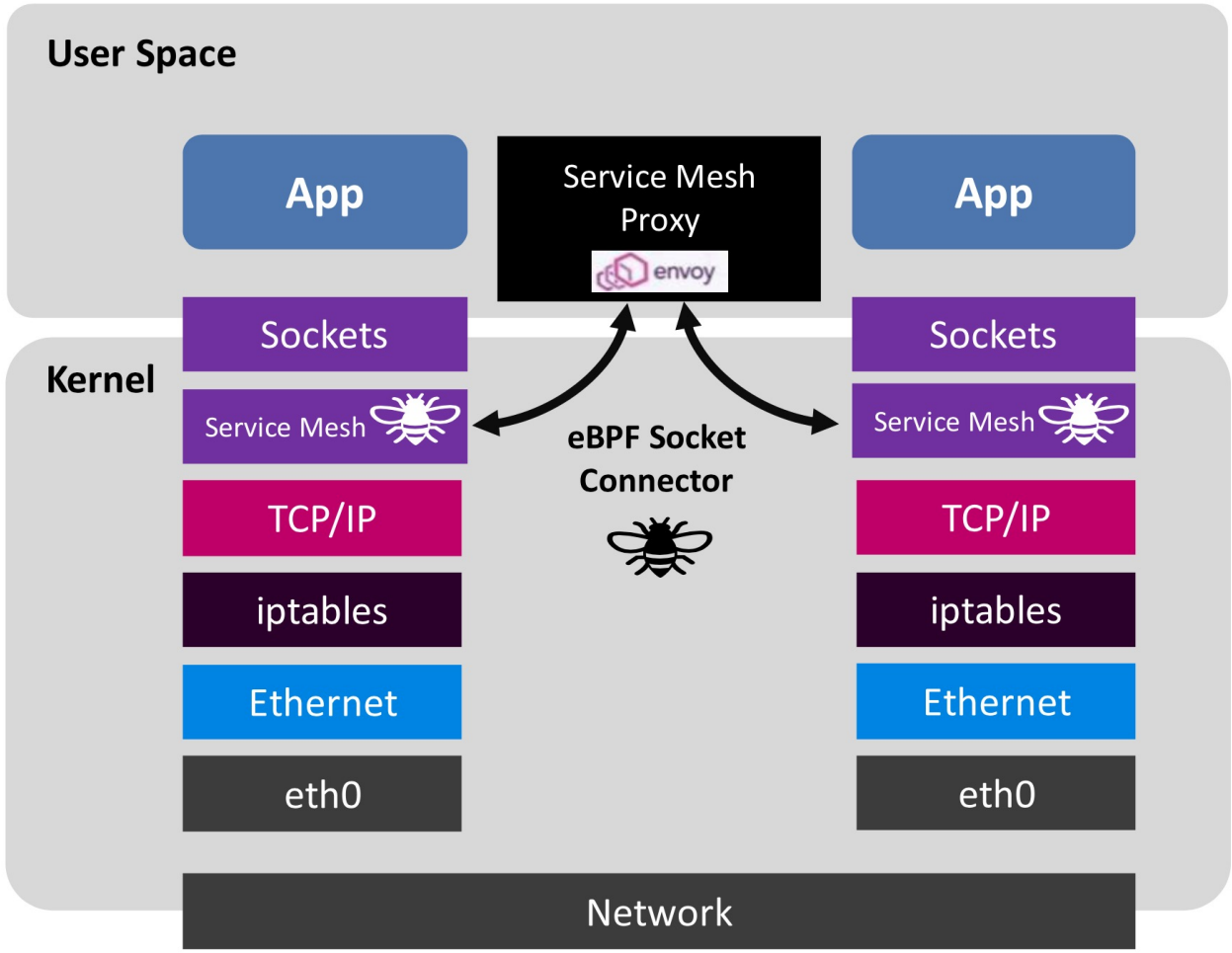
- 2.5x vs. regular Iptables Linux networking
- 4.3x over IPVS for load balancing
- O(n) to O(1) operation for looking up a rule

https://cilium.io/blog/2021/05/11/cni-benchmark/

How eBPF may reduce the number of *service mesh proxies* to provide the same services



N pods/node ➔ N proxies/node

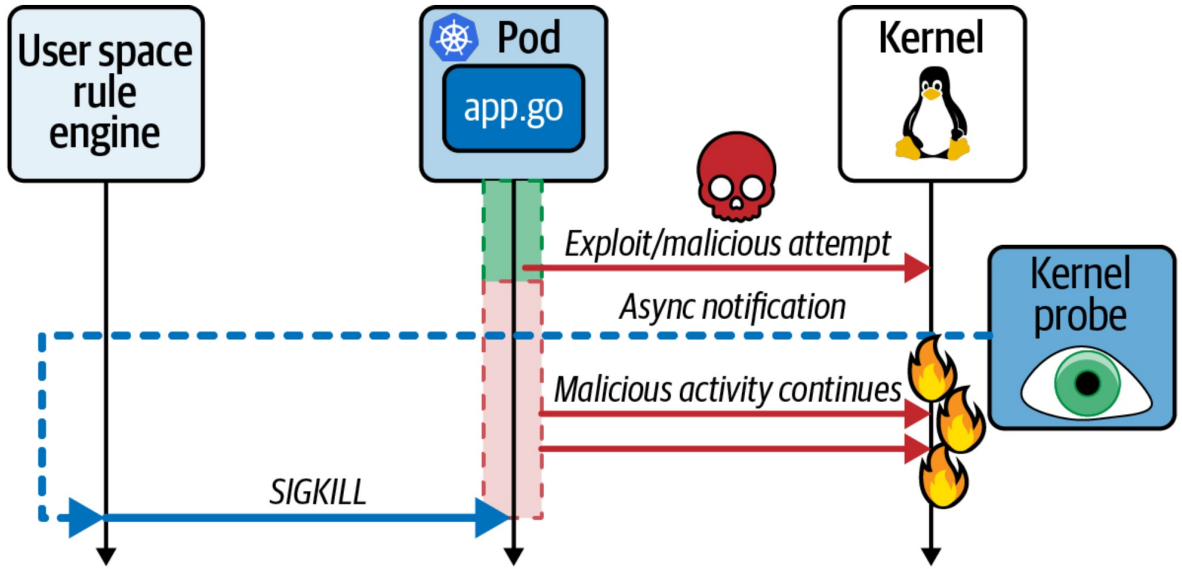


N pods/node ➔ 1 proxy/node

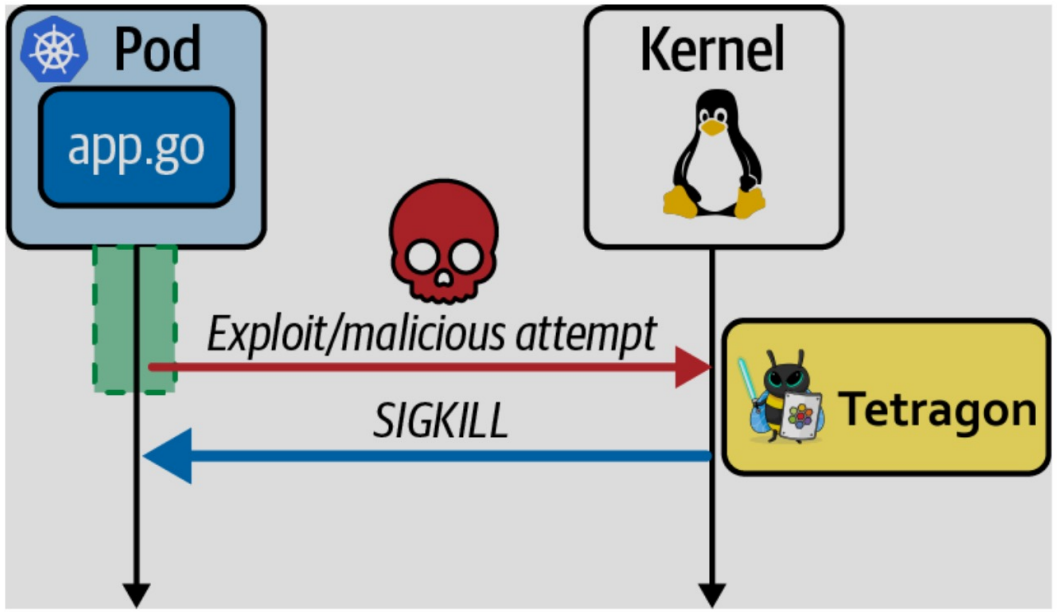
https://isovalent.com/blog/post/cilium-service-mesh/

eBPF for runtime security

An ***asynchronous notification*** from kernel to user space (rule engine) allows some time for an attack to continue



eBPF programs ***kill malicious processes synchronously*** by sending a SIGKILL signal from the kernel



Outline

The path to 6G

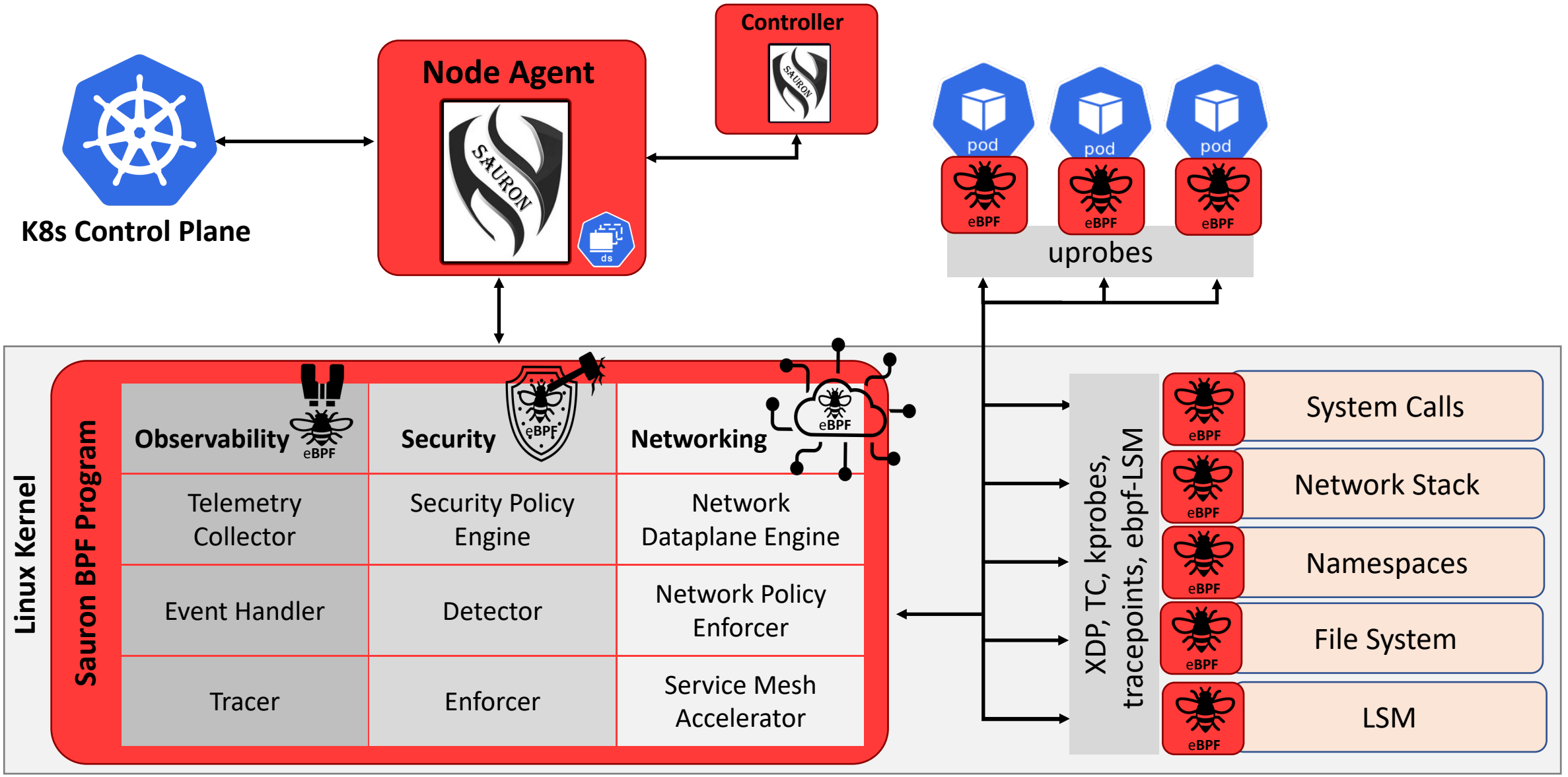
The powers of eBPF

eBPF for Kubernetes

Sauron eBPF platform

Conclusions

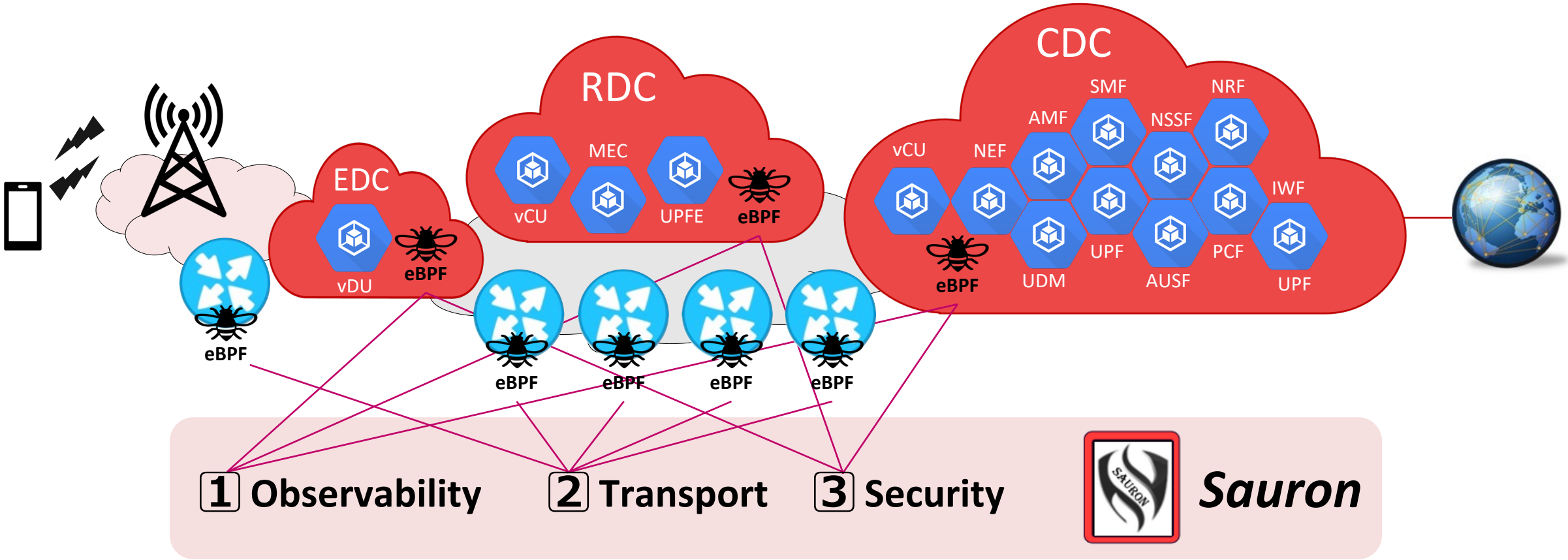
Sauron eBPF



https://ieeexplore.ieee.org/document/10138542

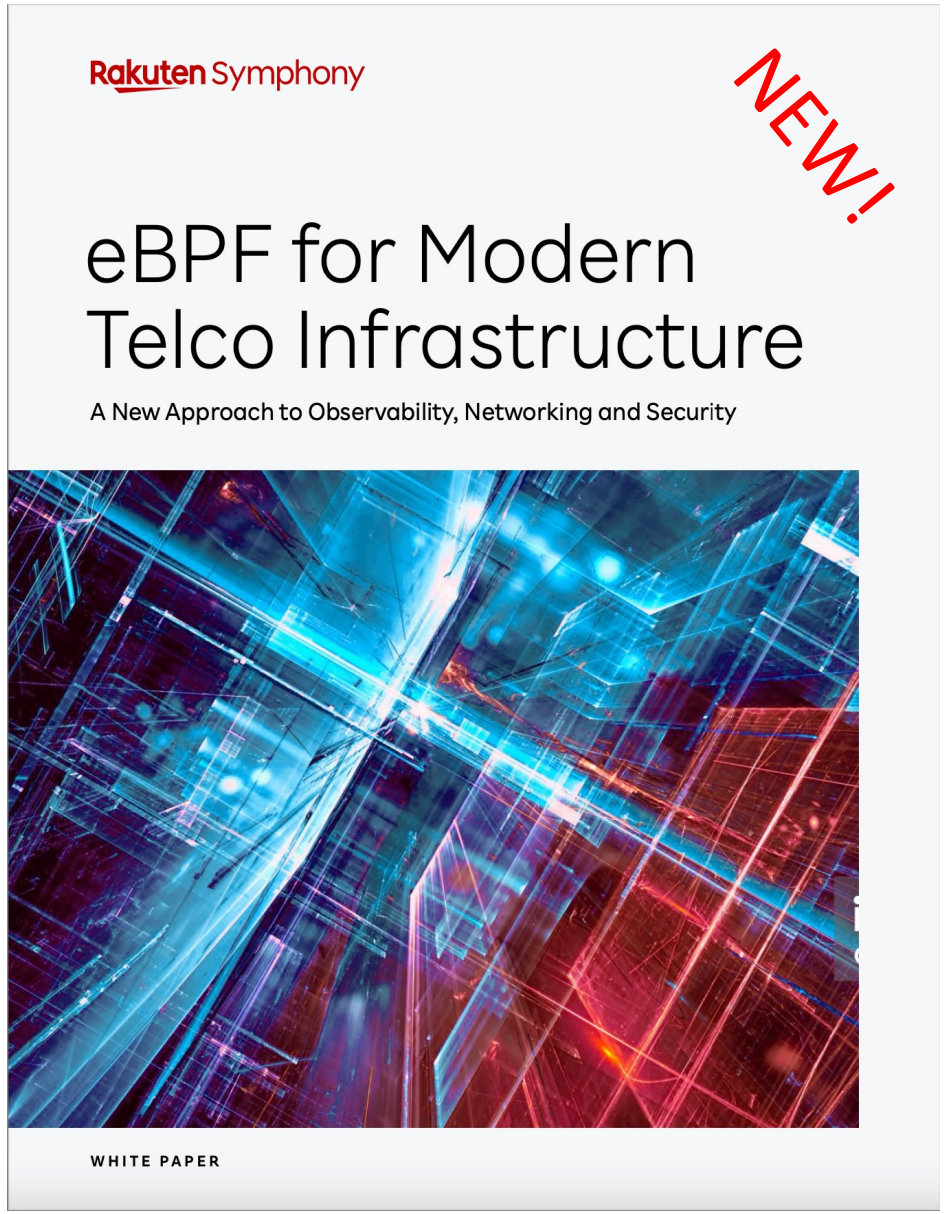
Sauron eBPF deployment

The extended Berkeley Packet Filter (eBPF) has the potential for networking (SDN of cloud native age and bridge cloud), observability everywhere and security assurance with improved QoE



https://ieeexplore.ieee.org/document/10138542

Rakuten papers



https://symphony.rakuten.com/

RESEARCH ARTICLE

eBPF: A New Approach to Cloud-Native Observability, Networking and Security for Current (5G) and Future Mobile Networks (6G and Beyond)

DAVID SOLDANI[1], (Senior Member, IEEE), PETRIT NAHI[1], HAMI BOUR[1], (Member, IEEE), SABER JAFARIZADEH[1], (Member, IEEE), MOHAMMED F. SOLIMAN[1], LEONARDO DI GIOVANNA[2], FRANCESCO MONACO[2], GIUSEPPE OGNIBENE[2], AND FULVIO RISSO[2], (Member, IEEE)

[1]Rakuten Mobile Inc., Setagaya-ku, Tokyo 158-0094, Japan
[2]DAUIN Department, Politecnico di Torino, 10129 Turin, Italy

Corresponding author: David Soldani (david.soldani@rakuten.com)

ABSTRACT Modern mobile communication networks and new service applications are deployed on cloud-native platforms. Kubernetes (K8s) is the de facto distributed operating system for container orchestration, and the extended version of the Berkeley Packet Filter (eBPF) – in the Linux (and MS Windows) kernel – is fundamentally changing the approach to cloud-native networking, security, and observability. In this paper, we introduce what eBPF is, its potential for Telco cloud, and review some of the most promising pricing and billing models applied to this revolutionary operating system (OS) technology. These models include schemes based on a data source usage model or the number of eBPF agents deployed on the network, linked to specific eBPF modules. These modules encompass *network observability*, *runtime security*, and *power dissipation* monitoring. Next, we present our eBPF platform, named *Sauron* in this work, and demonstrate how eBPF allows us to write custom code and dynamically load eBPF programs into the kernel. These programs enable us to estimate the *energy consumption* of cloud-native functions, derive *performance counters and gauges* for transport networks, 5G applications, and non-access stratum protocols. Additionally, we can detect and respond to *unauthorized access* to cloud-native resources in real-time using eBPF. Our experimental results demonstrate the *technical feasibility of eBPF* in achieving highly performant monitoring, observability, and security tooling for current mobile networks (5G, 5G Advanced) as well as future networks (6G and beyond).

INDEX TERMS eBPF, extended Berkeley packet filter, cloud-native observability, cloud-native security, cloud-native networking, cloud-native monitoring, 5G, 5G Advanced, 6G, Kubernetes, K8s.

https://ieeexplore.ieee.org/document/10138542

Outline

The path to 6G

The powers of eBPF

eBPF for Kubernetes

Sauron eBPF platform

Conclusions

Conclusions

- **Building on the existing network architecture:**
  Leveraging the current network architecture as a solid foundation for the development of 6G
- **Collaborative efforts for innovative 6G use cases:**
  With our Ecosystem Partners we are actively collaborating to explore and develop diverse 6G use cases, including logistics, smart factories, drones, medical applications, and more
- **Empowering a secure and cloud-native 6G ecosystem:**
  Utilizing Rakuten Symphony, we aim to create a robust and secure 6G ecosystem ***powered by eBPF technology***

References

1. D.Soldani, "*eBPF: A New Approach to Cloud-Native Observability, Networking and Security Tooling for Current and Future Networks*," Public Lecture, Dec. 2023.
2. D. Soldani, P. Nahi, H. Bour, S. Jafarizadeh, M. Soliman, L. Di Giovanna, F. Monaco, G. Ognibene, and F. Risso, "*eBPF: A New Approach to Cloud-Native Observability, Networking and Security for Current (5G) and Future Mobile Networks (6G and Beyond)*," IEEE ACCESS, Jun. 2023.
3. D. Soldani, "*eBPF for Telco*," Rakuten Symphony, White Paper, Mar. 2023.
4. D. Soldani, "*The Power of eBPF for Cloud Native Systems*," Cybersecurity Magazine, Dec. 2022.
5. D. Soldani, H. Bour, S. Jafarizadeh "*Security and Observability Implementation for Cloud Native Platforms*," Cybersecurity Magazine, Part1, Part2 and Part3, Sept. 2022.
6. D. Soldani, "*From security enhanced 5G networks to security by design 6G systems*," Cyber Australia, Oct. 2021.
7. D. Soldani, "*6G fundamentals: vision and enabling technologies - From 5G to 6G trustworthy and resilient systems*," The Australian Journal of Telecommunications and the Digital Economy (AJTDE), Sept. 2021.
8. D. Soldani, "*From Security-Enhanced 5G to Security-by-Design 6G*," Cyber Defense Magazine, Aug. 2021.
9. D. Soldani, "*6G Fundamentals: Vision and Enabling Technologies*," 6GWorld Research Paper, Jun. 2021.
10. D. Soldani, "*5G Security – Towards trustworthy products for resilient networks*," Cyber Defense Magazine, Feb. 2021.
11. D. Soldani, "*The potential of eBPF for cloud native systems*," Rakuten. Dec 2022.
12. D. Soldani, "*On recent cyber incidents in Australia,"* LinkedIn article. Nov 2022.
13. D. Soldani, "*Who'd keeping OPEN RAN secure?*", Rakuten. Oct 2022.
14. D. Soldani, "*Towards 6G Cloud Native and Secure by Design*," LinkedIn article. Sept 2022.
15. D. Soldani, "D. Soldani, "*6G starts with AI, open vRAN integration and ever increased security*," Rakuten. Aug. 2022.


Rakuten