ISOVALENT

The Future of eBPF-based Networking and Security

Thomas Graf
Co-Creator Cilium, CTO & Co-Founder, Isovalent

Why is eBPF the Future?

ISOVALENT

A bit of Networking History

Networking is almost entirely physical. Cables, perimeters, and a lot of L2.

A bit of Networking History

90s

Networking is almost entirely physical. Cables, perimeters, and a lot of L2.

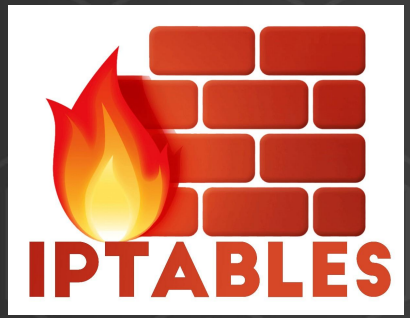
[The Sounds of Dialup Modems and Related Equipment]

SCAN ME

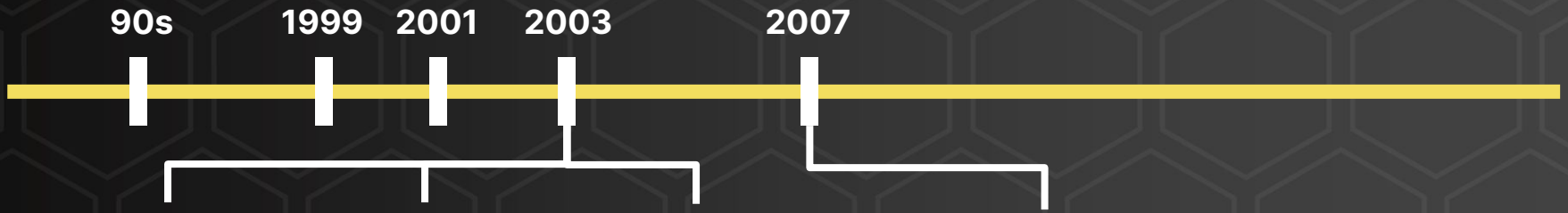
ISOVALENT

A bit of Networking History

Designed primarily to protect the host and to replace HW firewalls.



A bit of Networking History



VLANs are described in 802.1Q. Things are starting to become virtual.

First release of Xen hypervisor

EMC acquires VMware

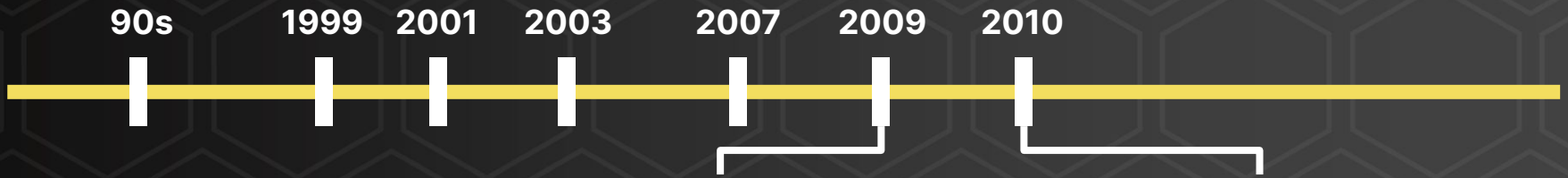
KVM hypervisor merged into Linux kernel

Networking for VMs is still mostly delegated to hardware with L2 bridges.

Start of Virtualization era

ISOVALENT

A bit of Networking History



First Open vSwitch release.

Early days of Software Defined Networking (SDN)

Programmability, Virtual Networks, and Overlays

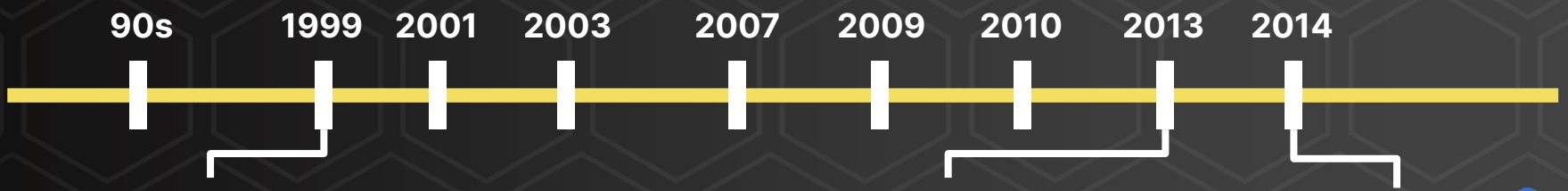
Massive move of networking from hardware to software.

First OpenStack Summit in Austin

Networking Virtualization Era

ISOVALENT

A bit of Networking History



iptables created by Rusty Russell as a successor to ipchains

Hello Docker

Networking is mostly inherited from VM era.

First commit to Kubernetes

High-level intent defined by users, fewer networking & security assumptions → lots of room for innovation.

BUT: Lots of iptables

The era of containers begins

ISOVALENT

How does eBPF fit in?

ISOVALENT

eBPF History

2014

First eBPF patch set is merged into the Linux Kernel.

ISOVALENT

eBPF History

eBPF backend merged into LLVM compiler suite.

cls_bpf makes Linux networking programmable

bcc project is announced

ISOVALENT

eBPF History

XDP is merged into the Linux kernel

Cilium project is announced

eBPF-based Networking, Security & Observability for Kubernetes and Cloud-Native environments.

Designed from scratch exclusively for eBPF.

ISOVALENT

eBPF's Fundamental Design Shift

Hardware Networking

- Functionality and scale is mostly predefined by hardware
- Long innovation cycles

Built for age of physical servers

Software Defined Networking

- Hardware networking concepts virtualized in software, e.g. virtual switches, virtual routers, ...
- Programmable flow tables
- Still based on IPs and Ports. No awareness of applications.
- Quicker innovation cycle due to software

Built for age of virtual machines

Cilium & eBPF Networking

- High-level intent translated into eBPF code, i.e., "networking-as-code"
- Networking is completely decoupled from security and visibility
- Understands security identies and application protocols (L7).
- Aware of applications while remaining transparent

Built for cloud-native age and Kubernetes

ISOVALENT

eBPF History

Brendan Gregg at Netflix shares **Linux BPF superpowers**

NETFLIX

Facebook shows **10x performance gain with BPF/XDP LB** over IPVS.

This is later released as Katran.

Katran

Cloudflare migrates **DDoS mitigation** from iptabels to BPF/XDP.

CLOUDFLARE

ISOVALENT

eBPF History

Cilium 1.0 is released

L3 Networking model, Native routing & overlay, Identity-based L3-L7 network security, ClusterIP Load-balancing

cilium

Cilium 1.2:

FQDN Policies, Multi-cluster networking

cilium

BTF is merged

The kernel becomes self-descriptive.

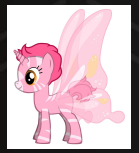
eBPF

ISOVALENT

eBPF History

2014 2015 2016 2017 2018 2019

bpftrace is announced



Cilium 1.4/1.5:

IPVLAN support, Transparent Encryption, eBPF templating

cilium

Cilium 1.6

Kube-proxy replacement, CNI chaining, Socket-based load-balancing, AWS ENI mode

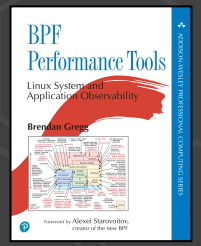
cilium

Hubble is released

Network, Service & Security Observability for Kubernetes using eBPF

HUBBLE

Brendan Gregg publishes "**BPF Performance Tools**" book



ISOVALENT

eBPF History

Cilium 1.7/1.8

XDP-based Load-balancing with DSR, Host Firewall, Session Affinity

cilium

Google announces eBPF & Cilium based Dataplane for GKE

Google eBPF

Cilium 1.9

Maglev Support, Bandwidth manager, Deny Policies, VM Support (External Workloads), TPROXY with eBPF, ...

cilium

ISOVALENT

What's next?

Edge Load-balancing with eBPF & XDP

Leverage speed, visibility and versatility of eBPF.

Projects:
Katran, Cilium, Unimog, ...

More Evolution into Application Awareness

Socket-based load-balancing, Intra-pod (k8s) network policies, Socket to socket networking

Combine network, system call and application protocol for ultimate threat detection and security

Metal & VM workloads

Connect modern containerized with metal & virtualized workloads.

Intergate the virtualized world and ease the transition.

eBPF-based ServiceMesh

Cilium already provides a lot of service mesh functionality.

Efficient, low cost, transparent, integrated into the operating system

ISOVALENT

Conclusion

We will see massive adoption of eBPF in the cloud-native world

Edge

- Load-balancing into k8s, VMs & Metal
- Visibility & Security

Kubernetes

- Networking (CNI)
- Service connectivity
- Network Policy
- Observability
- Multi-cluster

VM/Metal Fleet

- Identity-aware connectivity
- Represent a VM/metal as workload in Kubernetes

Host

- Melting of runtime and network security. Why differentiate between API and system calls?
- Application profiling and tracing
- System troubleshooting

ISOVALENT

Thank You!

cilium.io

github.com/cilium/cilium

ISOVALENT