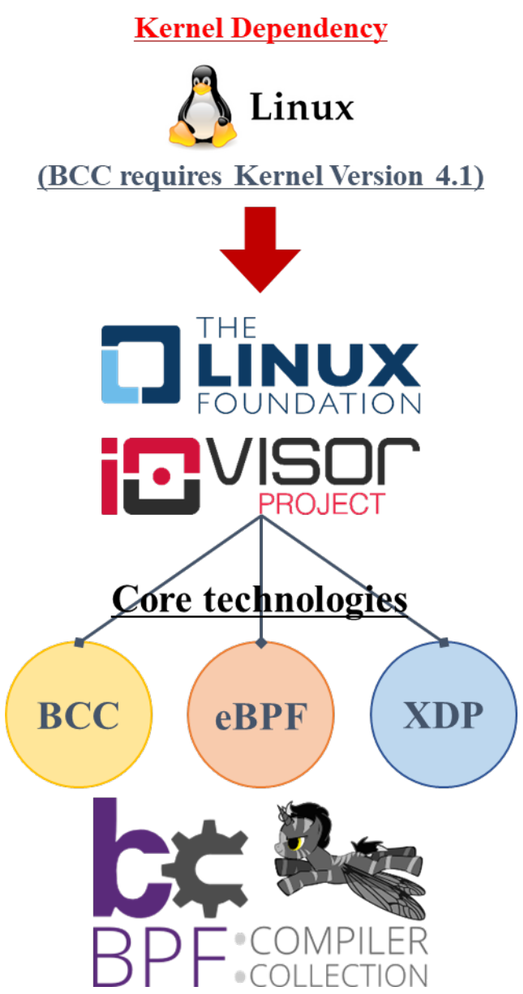
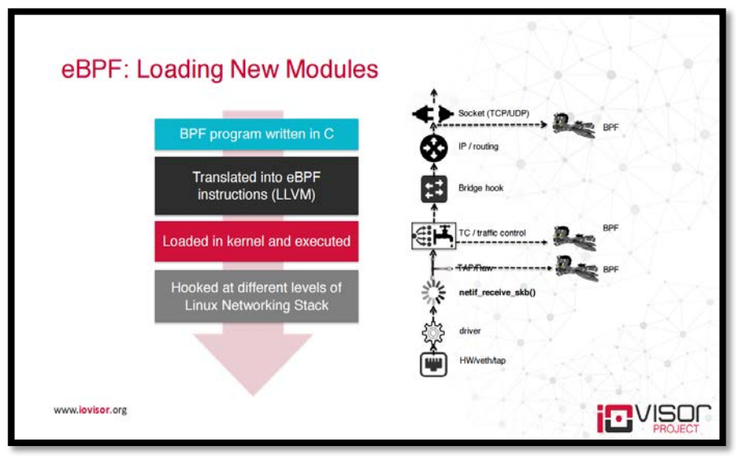
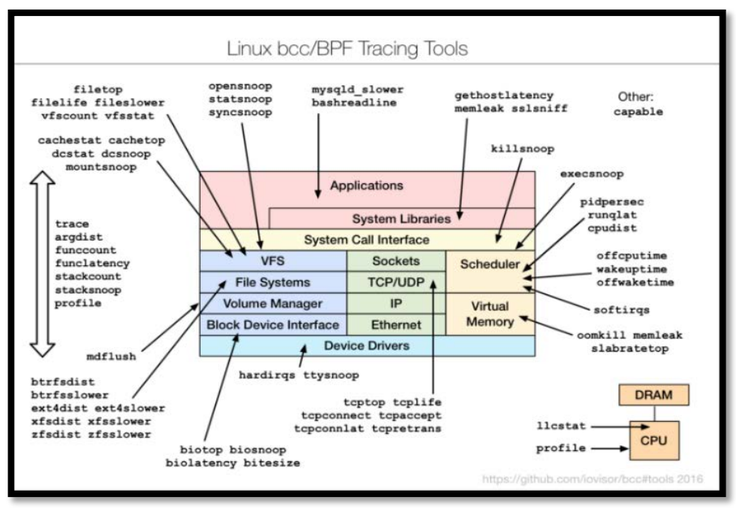
모니터링 기능 지원 가능한 IO Visor 기반의 Site Visibility Framework

NetCS Lab. (Networked Computing Systems Laboratory), GIST
Taekho Nam and JongWon Kim
{thnam, jongwon}@nm.gist.ac.kr

What is IO Visor?: Introduction of Open Source IO Visor Project







What is IO Visor?

An open source project to accelerate the innovation, development virtualized in-kernel IO services for tracing, analytics, monitoring, security, and networking functions.

eBPF (extended Berkeley Packet Filter)

- Originally created as a way to analyze and filter network packets for network monitoring purposes.
- Referred to as the universal in-kernel virtual machine.
- Designed to give ability to create any in-kernel I/O modules.

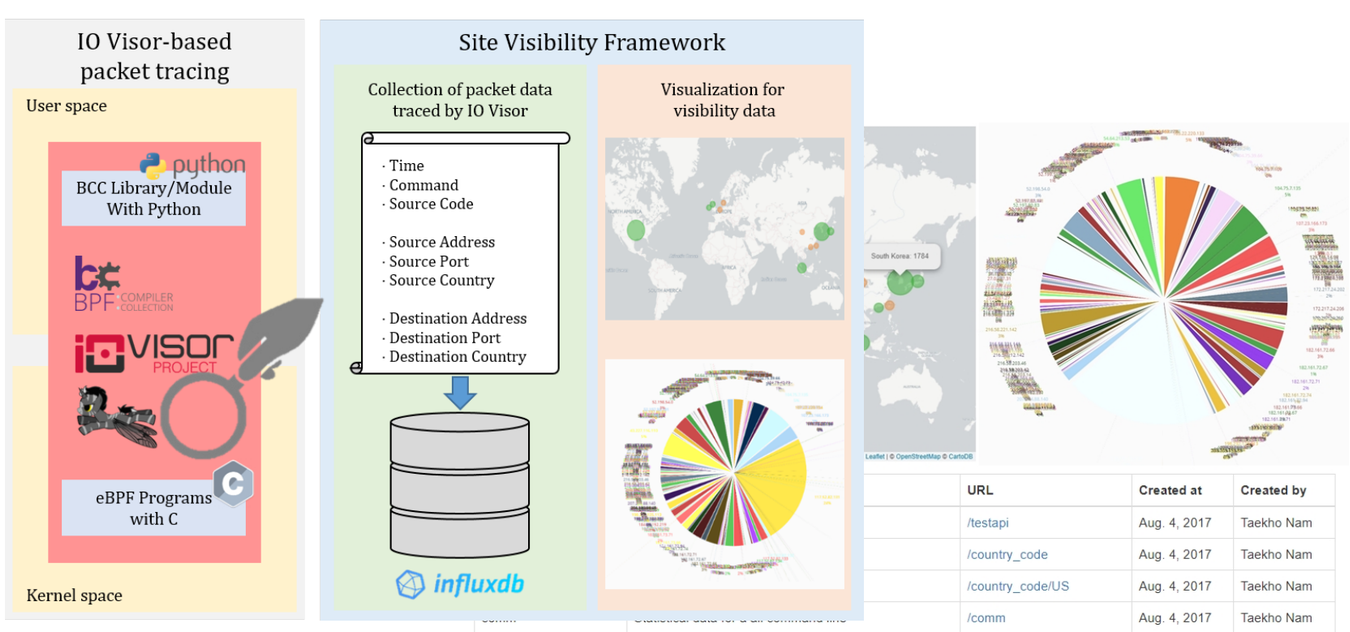
BCC (BPF Compiler Collection)

- BCC is a set of tools leveraging eBPF for kernel tracing.
- Make eBPF programs easier to write.

XDP (eXpress Data Path)

- Be implemented dynamically with the integrated fast path without kernel modification.
- XDP is a new function of IO Visor Project.

IO Visor eBPF/BCC-based Packet Tracing and Collection: Overview

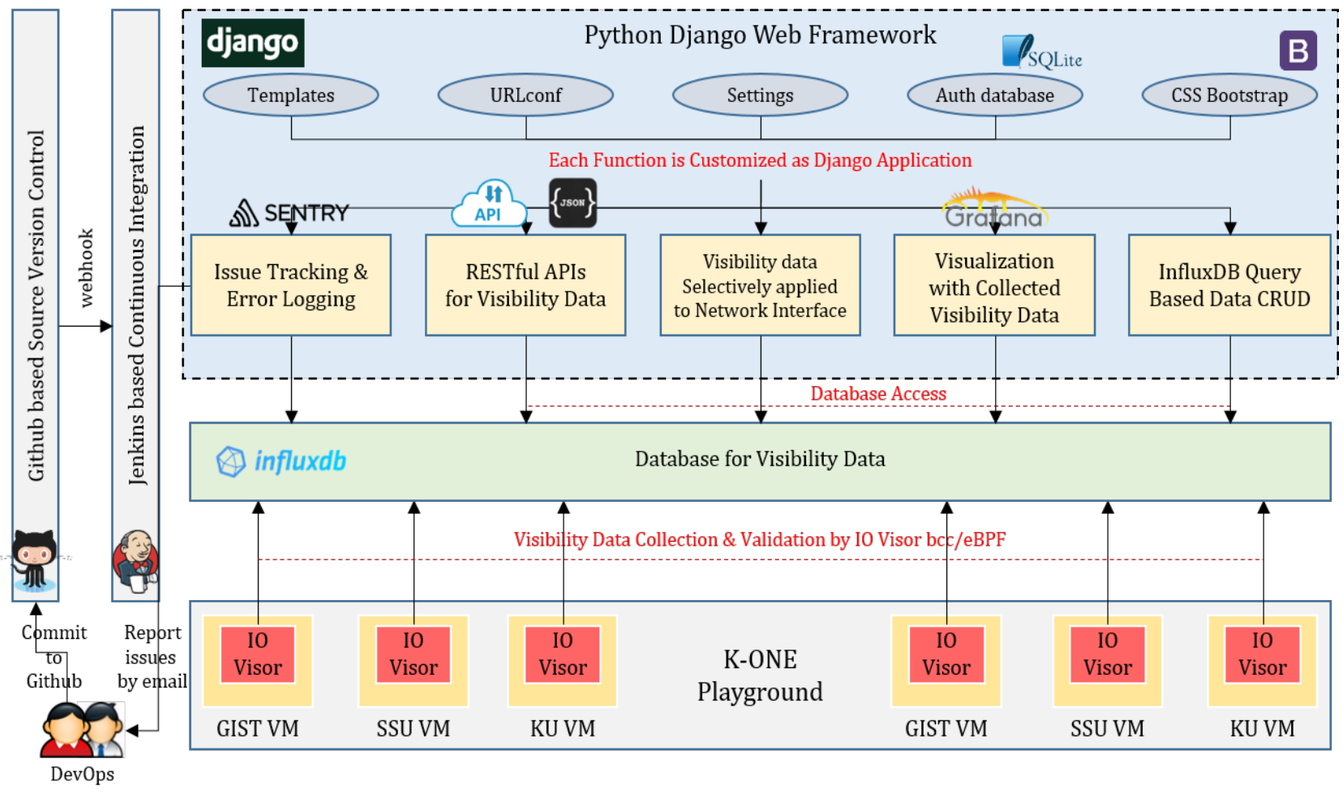


		URL	Created at	Created by
		/testapi	Aug. 4, 2017	Taekho Nam
		/country_code	Aug. 4, 2017	Taekho Nam
		/country_code/US	Aug. 4, 2017	Taekho Nam
		/comm	Aug. 4, 2017	Taekho Nam
comm/[a-zA-Z]+	Statistical data for a specific command line	/comm/http	Aug. 4, 2017	Taekho Nam
dest	Statistical data for a all destination address	/dest	Aug. 4, 2017	Taekho Nam
dest/[IPv4]{1}	Statistical data for a specific destination address	/dest/96.16.169.177	Aug. 4, 2017	Taekho Nam
source	Statistical data for a all source address	/source	Aug. 5, 2017	Taekho Nam
source/[IPv4]{1}	Statistical data for a specific source address	/source/210.117.251.34	Aug. 5, 2017	Taekho Nam
all	Visibility data containing all collected by IO Visor	/all	Aug. 6, 2017	Taekho Nam

IO Visor eBPF/BCC-based Packet Tracing and Collection

- The overview of packet tracing and collection based on eBPF/BCC to inspect all packets passing through the multiple network interfaces of Linux-based SmartX Box.
- When packets are entering and leaving the network interfaces of box (e.g., eth0), the kernel-space I/O networking is inspected with eBPF program.
- BCC programs extract the packet-level data from the header of traced packets.
- BCC programs also post-process the formatting of collected packet data and store it into InfluxDB
- Grafana-based visualization accesses visibility data stored in InfluxDB by passing the appreciate query

Preliminary Design for IO Visor eBPF/BCC-leveraged Site Visibility Framework



IO Visor for Site Visibility Framework

- A Django-based software framework that leveraging IO Visor eBPF/BCC-based packet tracing and collection.
- By utilizing packet data traced by eBPF/BCC, it can support the visibility visualization of traced packets and provide associated RESTful APIs.
- All components in the site visibility framework are wrapped by Django web framework and thus inherit the core components.
- By adopting DevOps-based automation concept, it can support continuous integration and issue tracking.
- These components are useful in providing visibility information for site operators to securely manage multiple clustered boxes, which is then helpful in overcoming the difficulty of resource and security management.