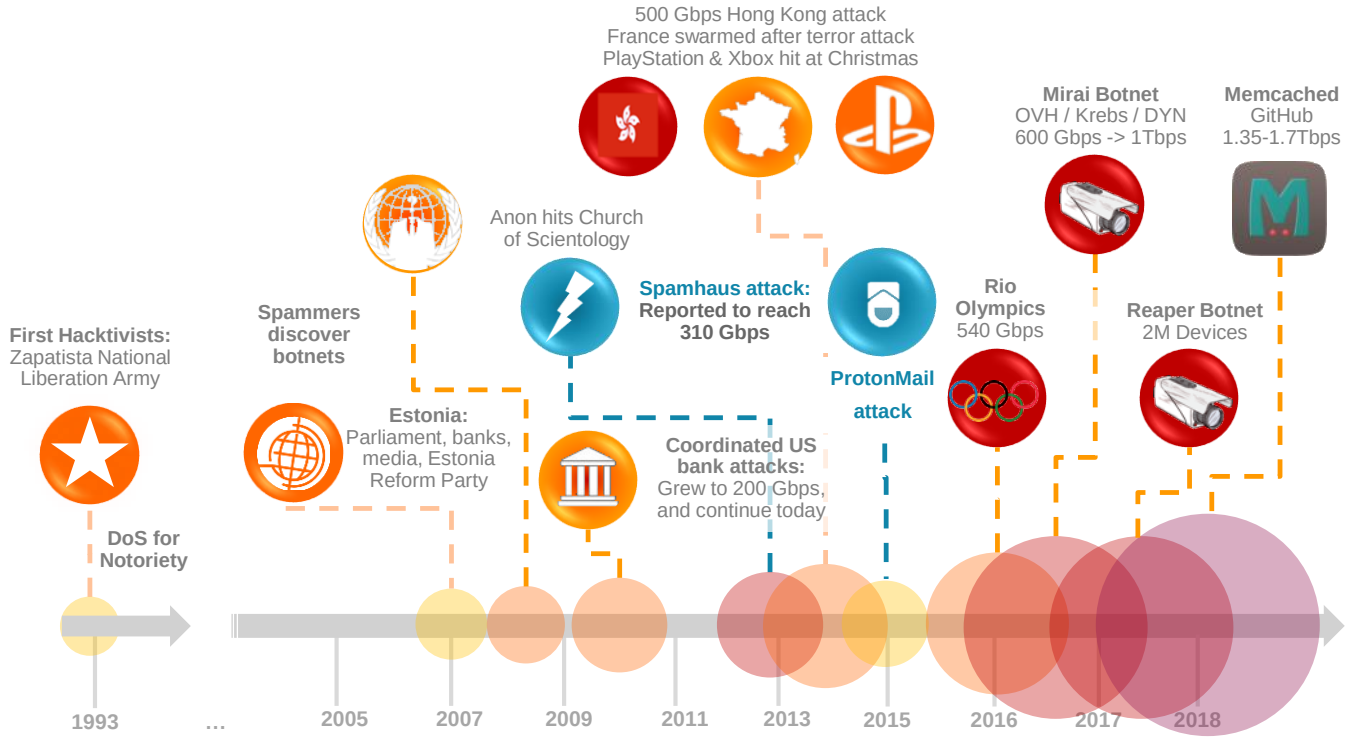
High Performance & NFV Packet Processing

Julian Palmer
Vice President, Engineering

Welcome to Edinburgh – Corero's R&D Base!

DDoS is Still on the Increase…



…and Small Attacks Dominate and Risks Evolve

New Vectors Still Appear…

World's biggest DDoS attack record broken after just five days

Memcached attacks are going to be this year's thing

The Register® Biting the hand that feeds IT

Infrastructure[+] & Business at Risk[*]

- 70% of UK Critical Infrastructure could be liable for fines under new EU NIS Directive
- 42% say DDoS "erodes customer trust", if public
- 26% say DDoS risks security of data or systems

[+] *Corero Freedom of Information Study, May 2018*
[*] *Corero DDoS Study of 300 IT professionals, Corero blog, August 2018*

corero

High Performance & NFV Packet Processing

Network Evolution - Show of Hands…

1. How many here have a 100G deployment strategy?
   - Researching
   - Underway or In Production
   - Future, i.e. 2+ years away
2. Anyone have an SDN and NFV strategy?
   - Researching
   - Underway or In Production
   - Future, i.e. 2+ years away
3. What environments are you focused on for SDN or NFV?
   - VMWare
   - KVM
   - Public Cloud (AWS, Google Cloud, Azure…)

Corero's Journey to Scale & Flexibility

- Challenges posed by Evolving Network Architectures:
  - Scaling 10Gbps line-rate protection to 100Gbps
  - Delivering the same DDoS protection in S/W on commodity H/W
  - Extending line-rate capability to virtualised (NFV/SDN) networks

- Key High-Level Objectives:
  - Could we develop a line rate 100G DDoS appliance on commodity H/W
  - Could we develop a portable software VM of Corero's DDoS protection
  - Could that VM deliver 10G line rate performance on commodity H/W

- How did we go about it?...
  - We are a software, not a hardware specialist
  - We need a common platform architecture

Requirements for Today's DDoS Protection

Accuracy **Surgical protection** with near **zero false positives**

Real-Time Block **automatically**, for **immediate** zero-touch protection

Reliability **Redundant** HW deployments, **Do No Harm** protections

Visibility Comprehensive attack **visualization** and **forensics**

Requirements for Today's DDoS Protection

Accuracy **Surgical** protection with near **zero false positives**

Real-Tin ion

Reliabili s

Break these and defence is as bad as the attack, or worse!

Visibility Comprehensive attack **visualization** and **forensics**

Primary Technical Challenges

1. A common s/w architecture capable of high performance & portability
2. Virtual machine and framework performance overheads
3. H/W capable of 100G line-rate, with DDoS protection workload

- Delivering the attributes needed for today's multi-vector DDoS attacks:
  - Always-on inspection with automatic blocking
  - Highly accurate volumetric DDoS protection, with sub-second response
  - Designed for worst-case packet loads and autonomous decision making
  - Do no harm approach to protect traffic when decision is uncertain

100G Line-Rate, with Commodity NICs?

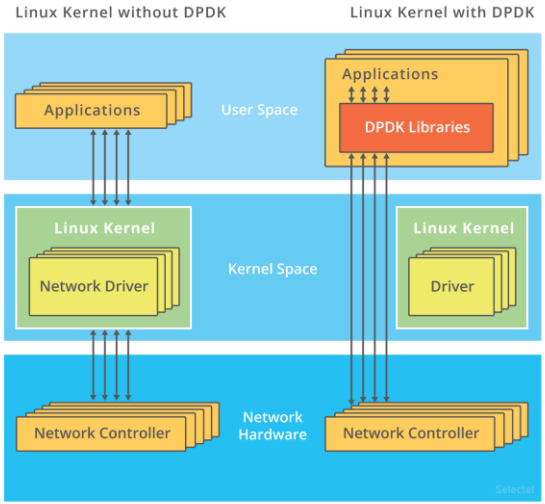
100G NIC comparison, using single Xeon E5-2658v4 @ 2.30GHz, 14 cores running DPDK software

- Investigated commercial 100G NIC cards, using DPDK:
  - Not line-rate at small packets, and some are lossy – a non-starter for DDoS protection
  - Some had PCIe efficiency issues, others could not achieve line rate at any packet size
- Alternatives exist, but all tie to a specific hardware vendor & software:
  - FPGA accelerated NICs, multicore Network Processors, network switch silicon, …
- Corero Conclusion:
  - Still need specialist H/W for 100G line-rate small packet sizes

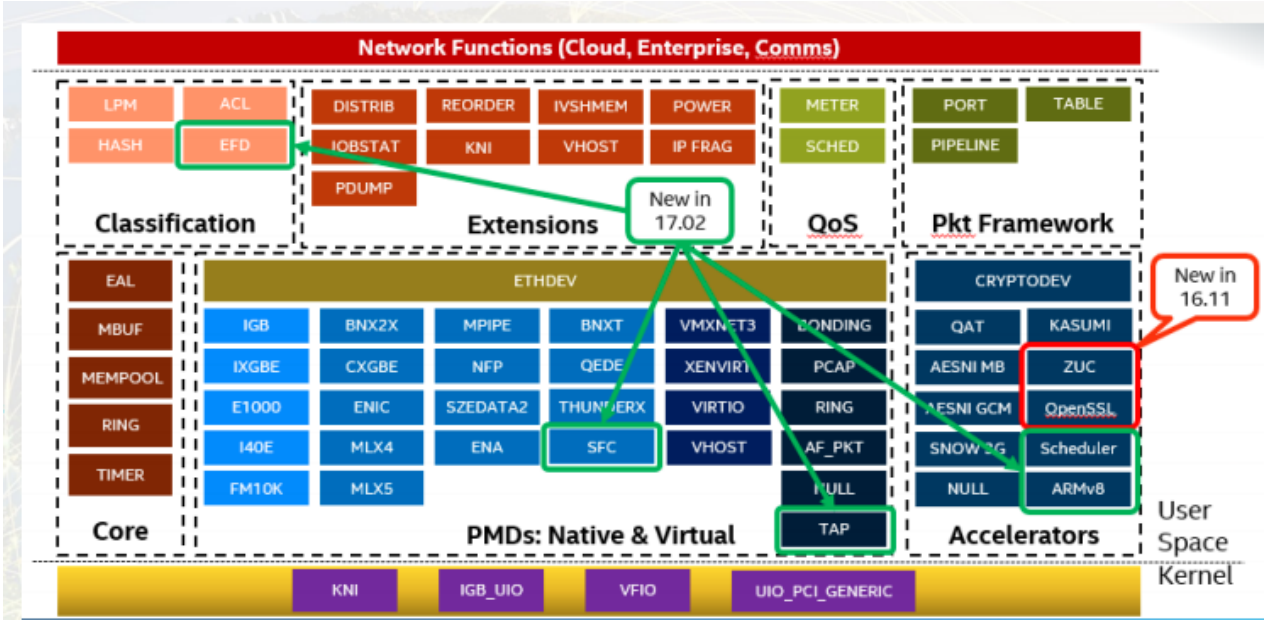
100G Line-Rate, on Intel, in Software?

- Data Plane Development Kit (DPDK) fitted our needs
  - Existing experience
  - High speed packet processing, in Linux userspace, bypassing kernel stack
  - Open source industry standard, with broad support and active development

- In DPDK ports are unbound from Linux
  - ifconfig does not see them
  - Application interacts directly with the hardware (via DPDK PMD)

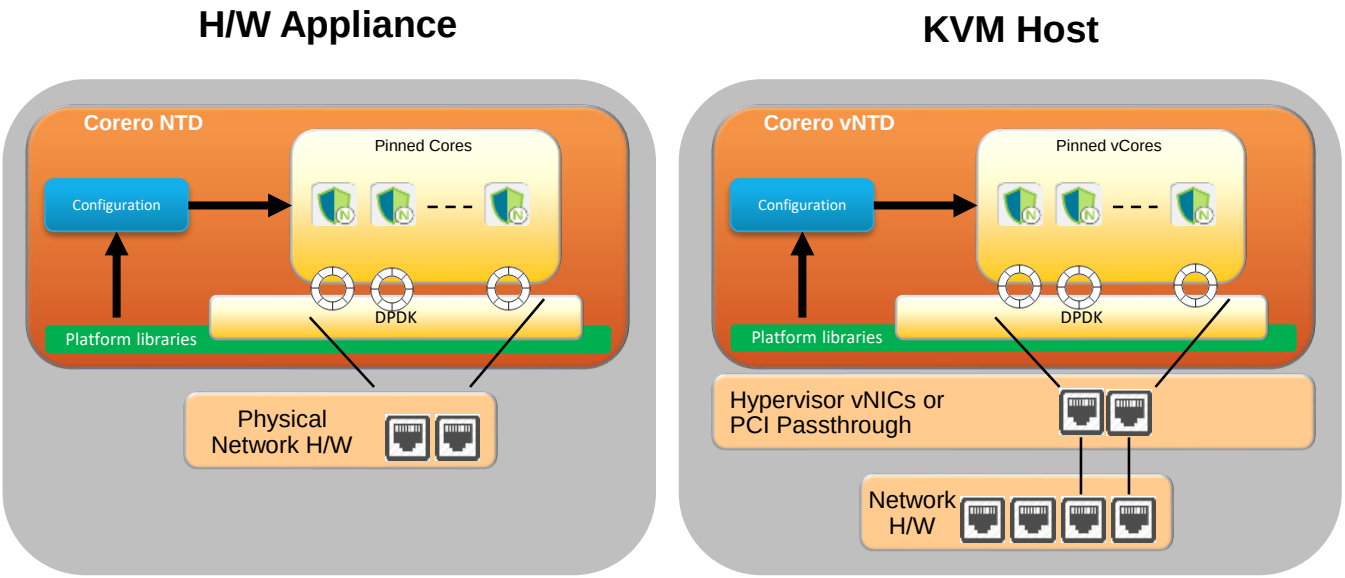


DPDK Offers a Broad and Active Ecosystem



- Ability to use a variety of extensions and PMDs gives a rich environment

DPDK Abstraction Enables Run Anywhere Goal



- Performance characteristics and platform libraries differ

Conclusions & Lessons Learned

- **Is line-rate 100G DDoS protection possible on commodity H/W?**
  - Yes, but with specialist NIC hardware needed for line-rate with small packets
  - Requires built for purpose software design, with high speed data path innovations
  - More cores increases contention, eventually losing performance
- **Can DDoS protection be made portable to Virtual platforms?**
  - Yes, Corero code is 95% the same between H/W and S/W forms
  - DPDK enables abstraction to integrate with H/W & Hypervisors
- **Could a DDoS Protection VM deliver 10G line-rate performance?**
  - Yes, VM runs @10G line rate (15Mpps bi-directional) on 8 vCPU cores
  - Efficient core use requires a built for purpose design and careful tuning
- **Getting close to line rate is relatively easy… getting to 100% line rate is hard**
  - Small issues get magnified in a system close to the edge

corero

Thank You!