Securing PaaS Docker & Weave

David Pollak

Devoxx.pl, June 2015

About @dpp

- Founded Lift, wrote Beginning Scala
- Wrote a bunch of spreadsheets
- Former CTO/VPE Cenzic (security)
- Lawyer by training, user of many technologies

Structure

- Mechanics
- Philosophy
- Discussion

Mechanics

Why?

- Built an analytics service
- Users upload code
- Code runs on isolated Spark clusters

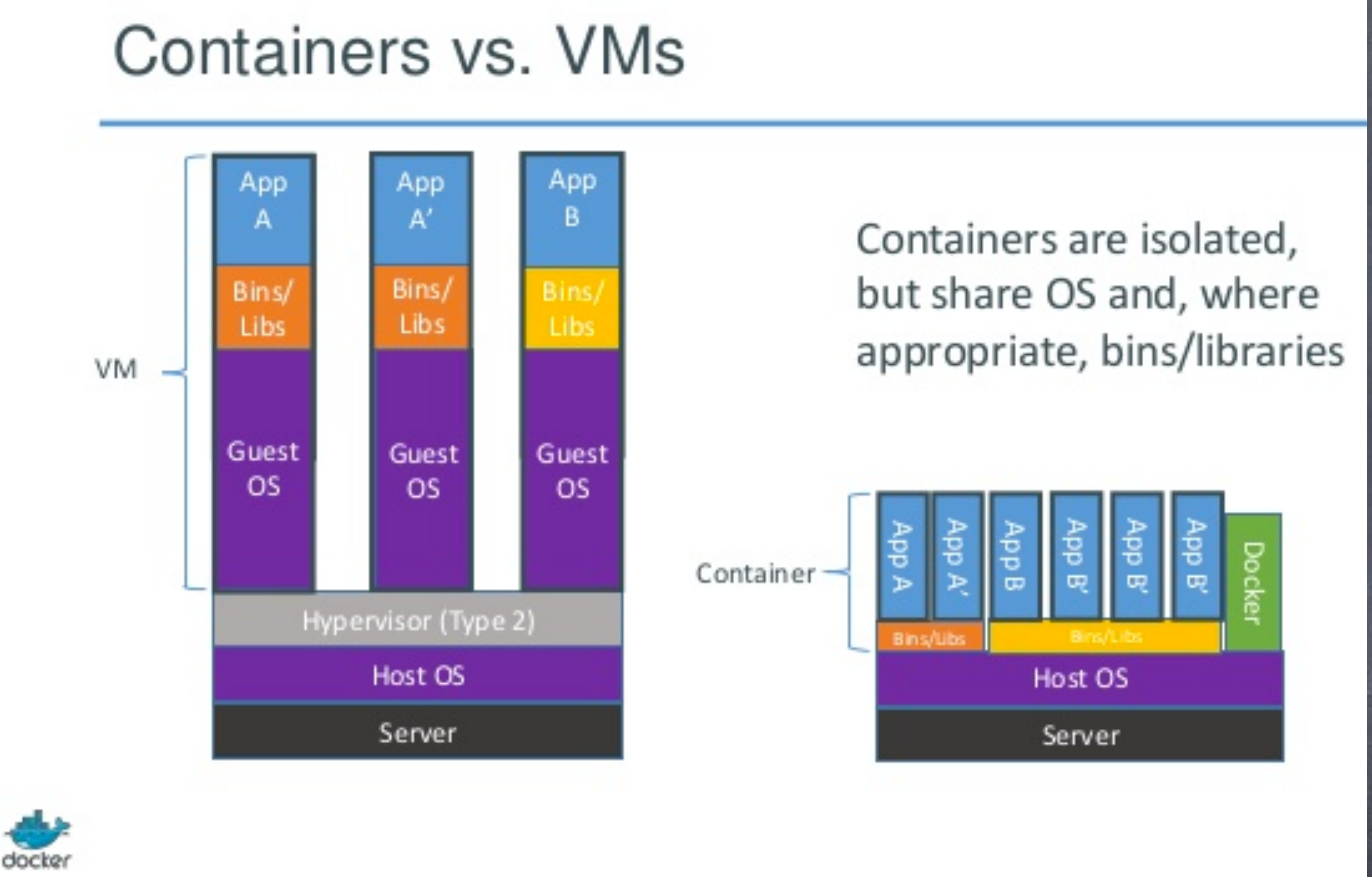
Threat Stories

- Discover competitor's data
- Discover competitor's analytics
- DoS competitor's systems

Docker

- Isolates Linux Processes & Libraries
- Inside it's like a machine/VM
- Fast Startup
- Simple Definition
- Excellent UI on top of lxc containers

Docker



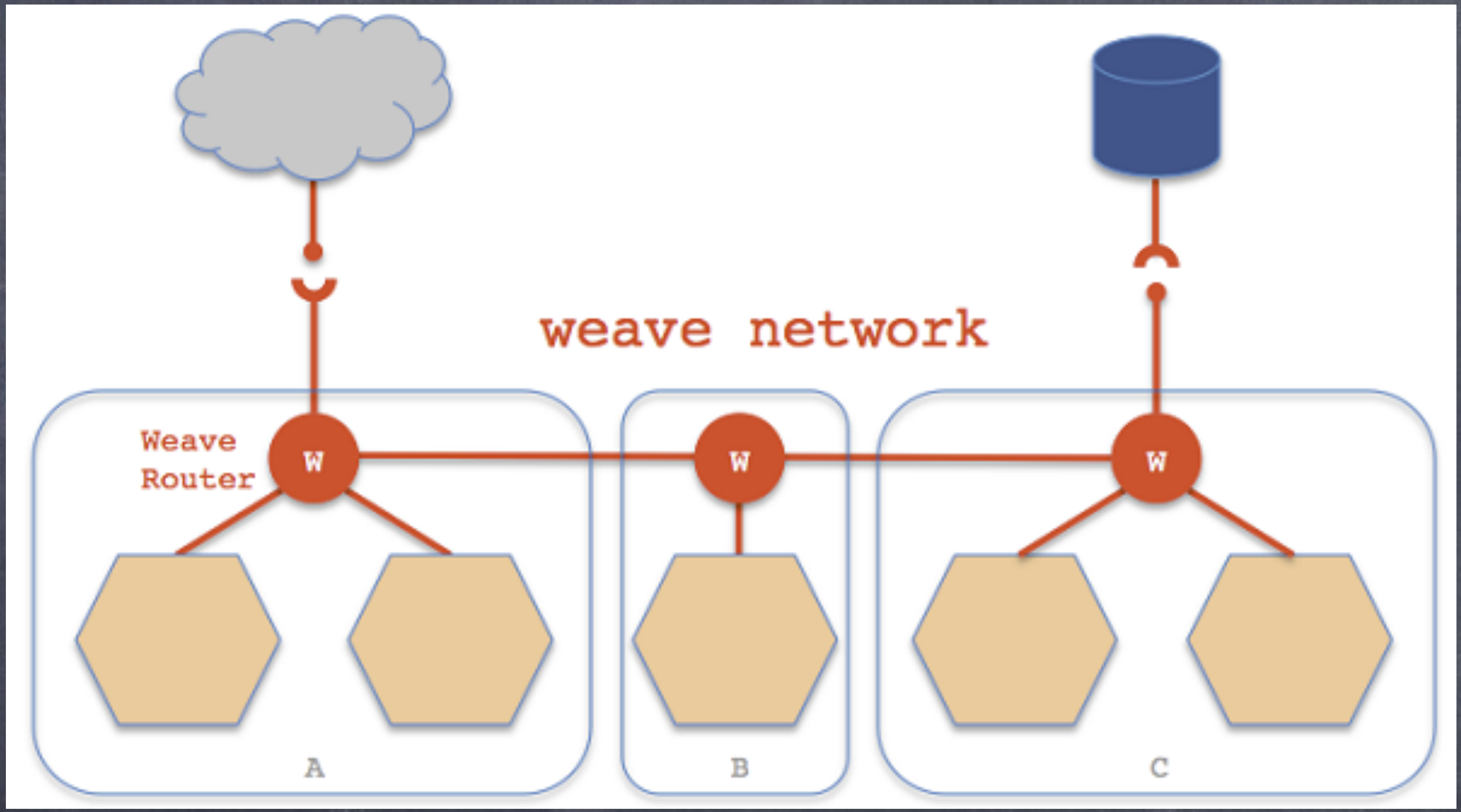
Containers vs. VMs

Containers are isolated, but share OS and, where appropriate, bins/libraries

Weave

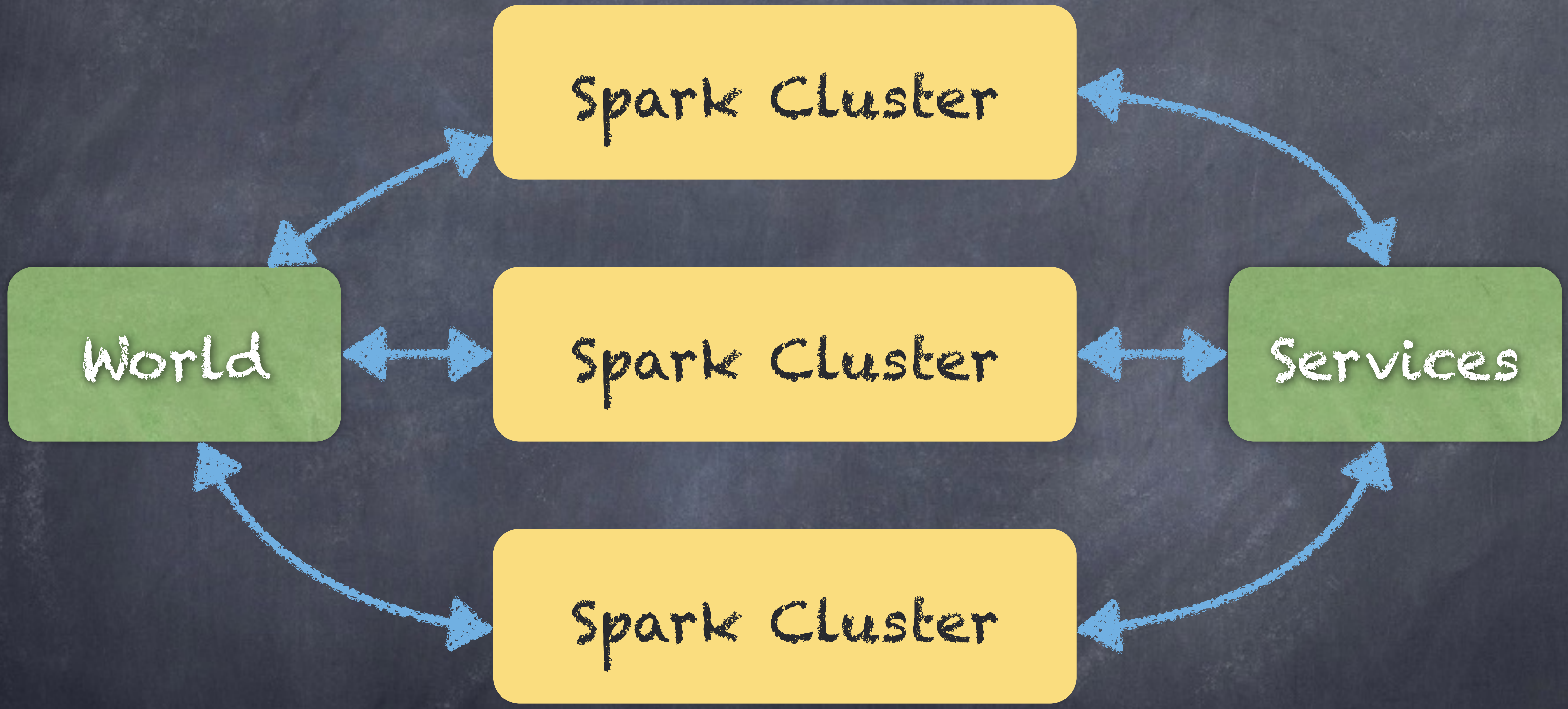
- http://weave.works
- Virtual Network Layer
- Works across hosts, seamlessly

Weave



Securing my PaaS

Big Picture



World

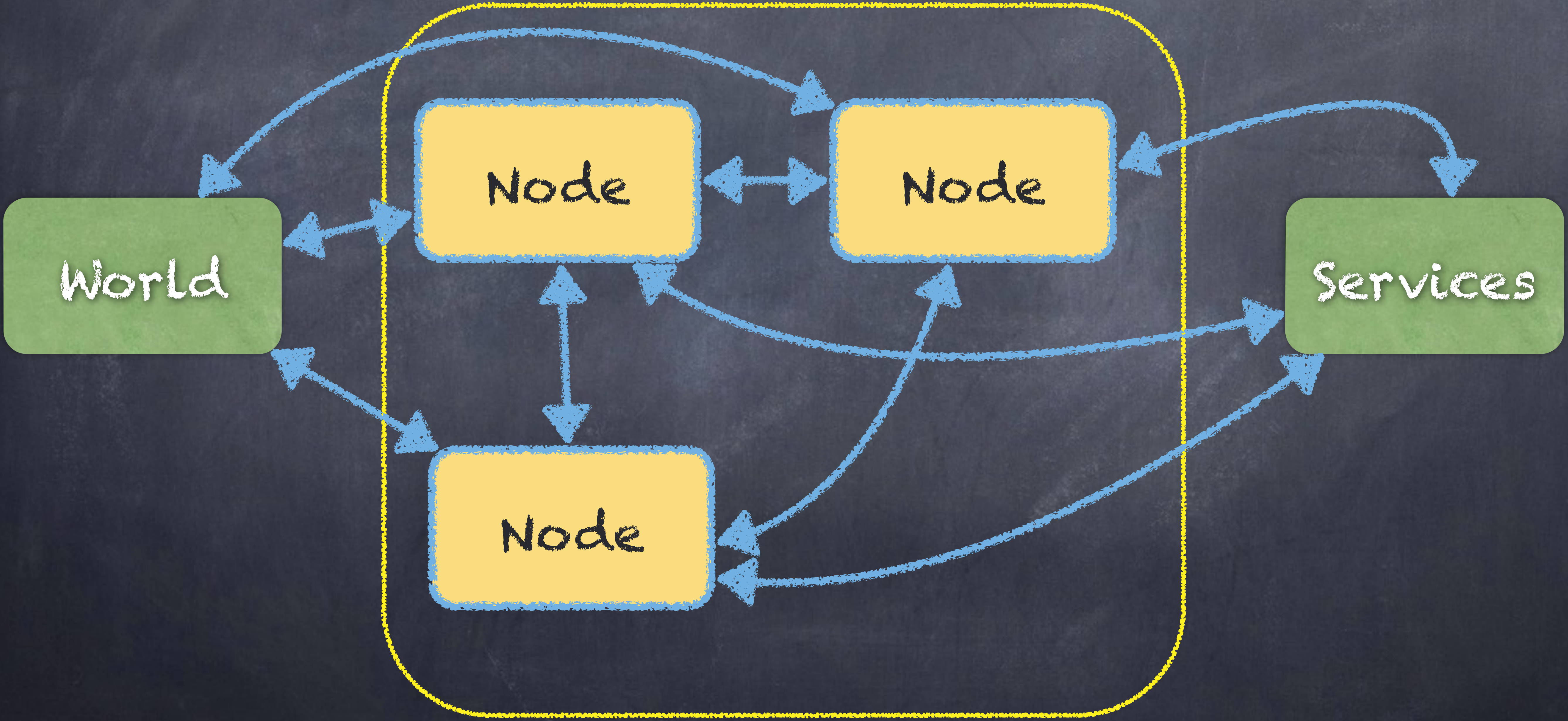
Spark Cluster

Spark Cluster

Spark Cluster

Services

Inside each cluster



World

Node

Node

Node

Services

Security & Threat Models

- Threats:
  - App to host via code
  - App to host via network
  - App to app via network
  - App to shared services
- Docker instances reasonably well isolated from host
- Weave subnets isolate cluster networks
- Services: HTTP only & Credentials

Clusters can See

- Nodes within Cluster
- World
- Services

Clusters cannot see

- Other Clusters
- Docker hosts

Clusters may span hosts...

Multiple clusters per host...

Docker

- Constrain what contents of container can do
- Start by disallowing networking
  `-net=none`
- Limit memory and swap:
  `-m 300M --memory-swap 300M`

Docker

- Defaults okay for:
  - CPU
  - Disk (10G limit)
  - etc.

Untrusted Containers

- Only communicate via HTTP/HTTPS
- Trusted HTTP proxies added: Squid

Networking

- Assign each cluster a /24 network
```
weave attach 10.4.1.3/24 mynode
```

- Add Squid into the network
```
weave attach 10.4.1.240/24 squid
```

- Nodes (across hosts) talk via Weave

Demo Time

Philosophy

Notable Security Failures

- FREAK
- Heartbleed
- Shellshock
- Target CC Loss: an SQL Injection
- Failures to interpret data

OWASP Top 10

- Injection: occurs when an application sends untrusted data to an interpreter
- XSS: occurs when an application includes user supplied data in a page sent to the browser without properly validating
- CSRF: allows the attacker to force the victim's browser to generate requests the vulnerable application thinks are legitimate requests from the victim.

NEVER trust what's on the wire!!

What if what's on the wire is Turing Complete?

Turing Complete

==

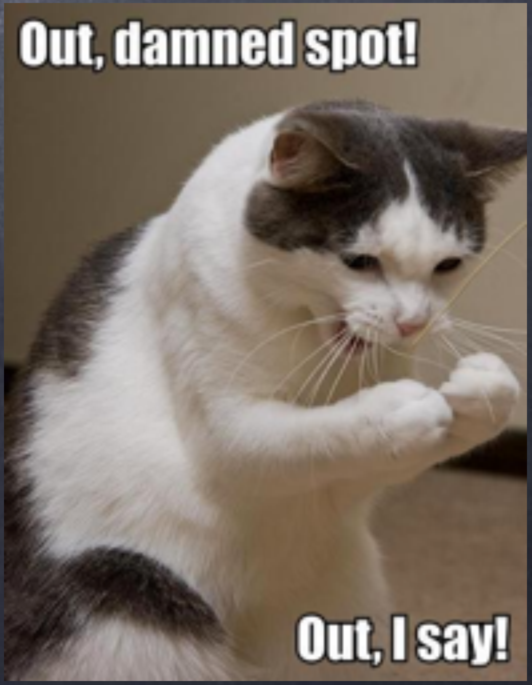
Executable Code

Turing Complete

- Magic: The Gathering
- MediaWiki Templates
- Apache Rewrite Rules
- Excel Yes! Excel!

"Real" Programs

- If it's Turing Complete, it can do anything
- No matter what you think, securing Turing complete is hard
- Out damned spot:
  you can't "clean" the program



Finding the right place to secure things is key

Let's talk Securing Things

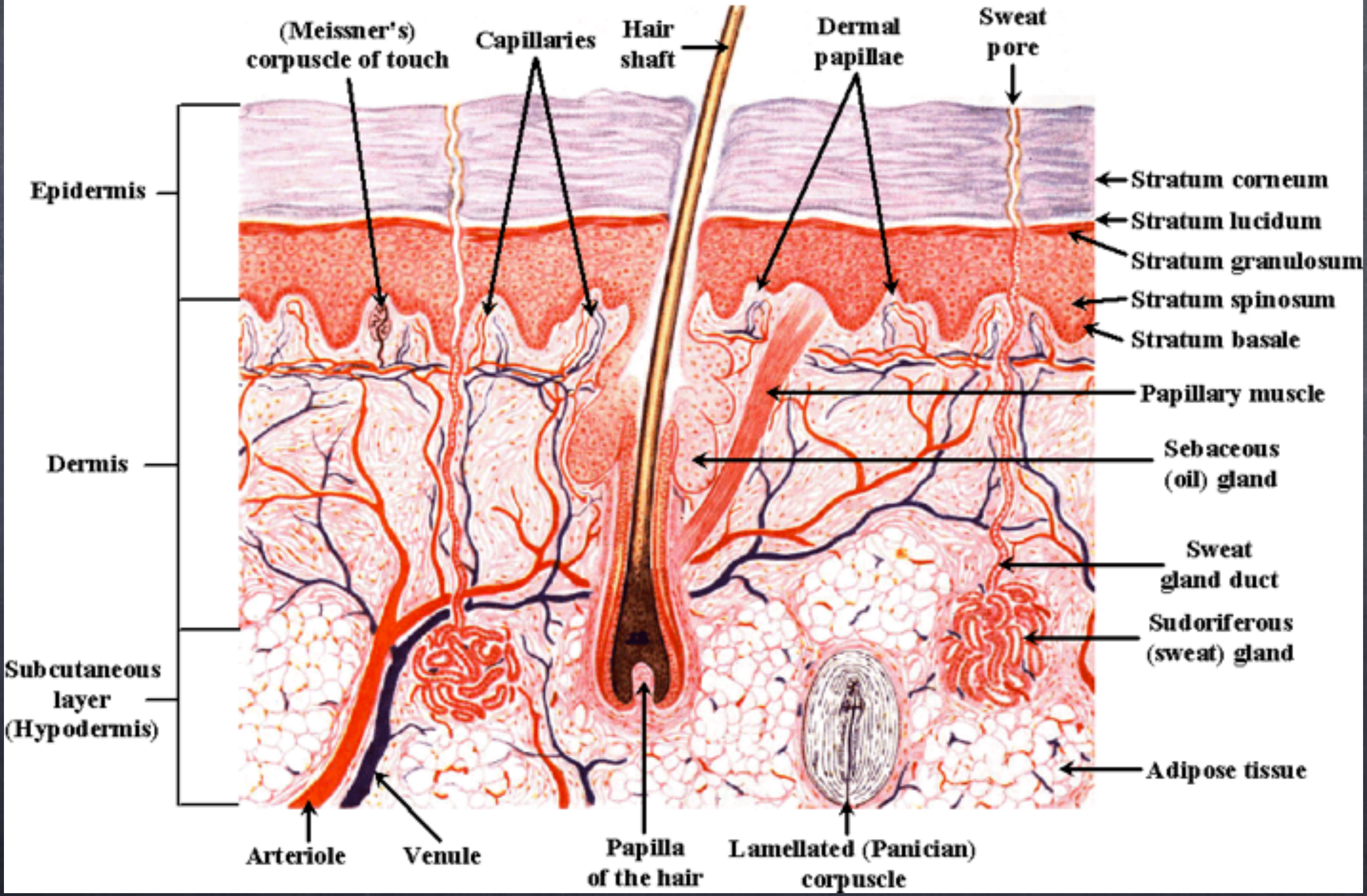
How do you truly secure data?

- Add a lot of entropy

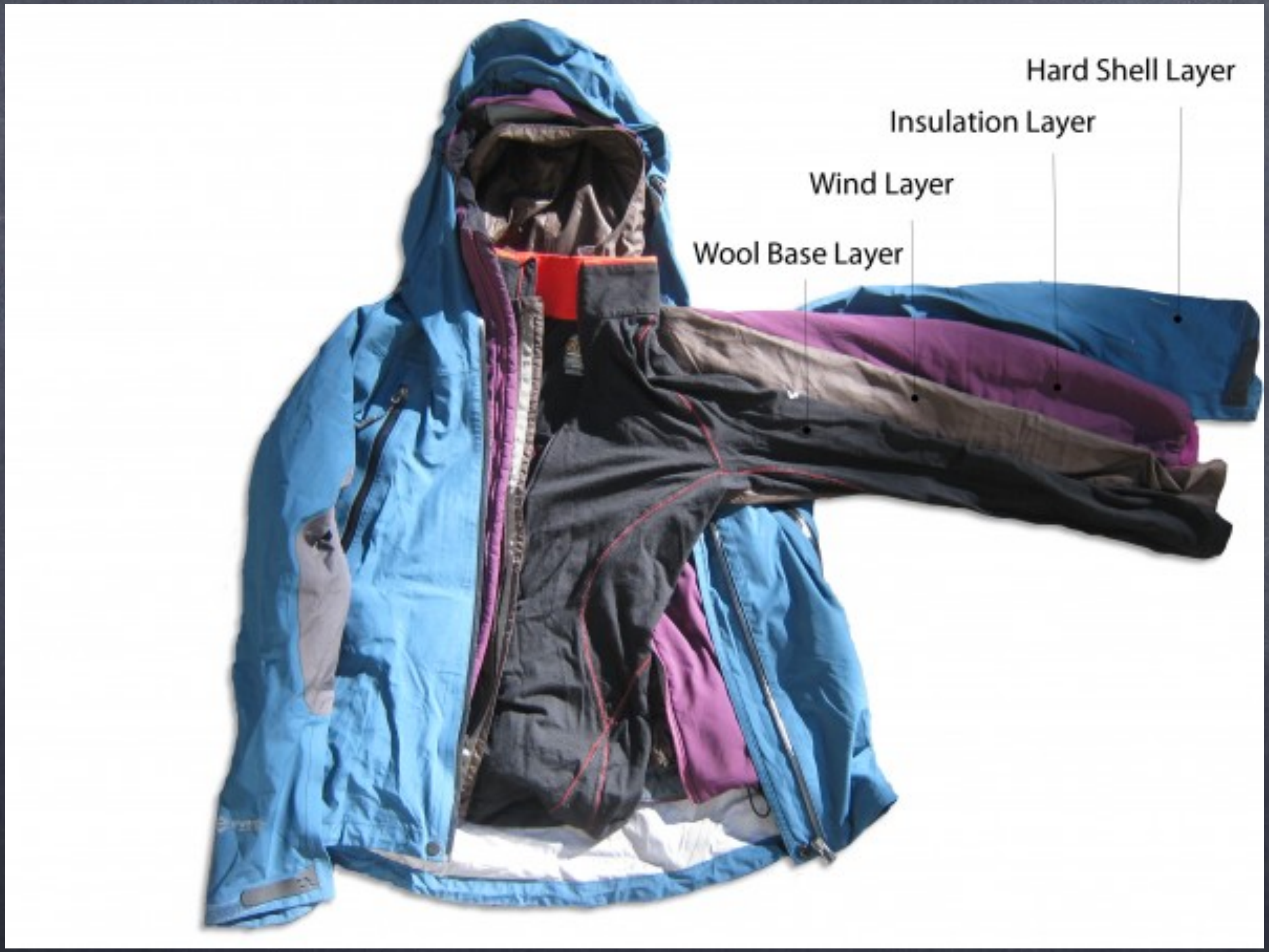
How do you secure data and make it accessible?

Layers!

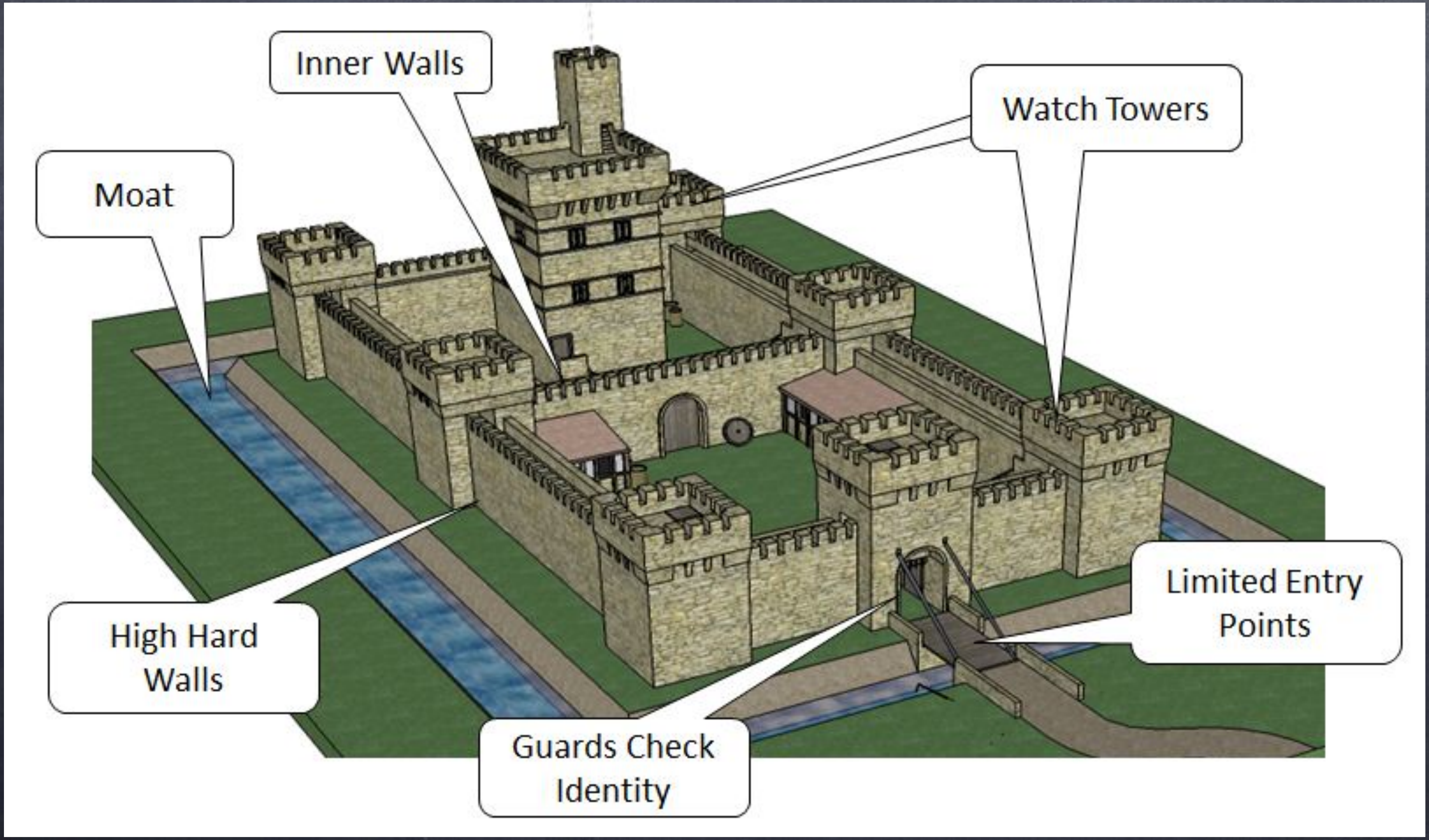
Layers in Biology



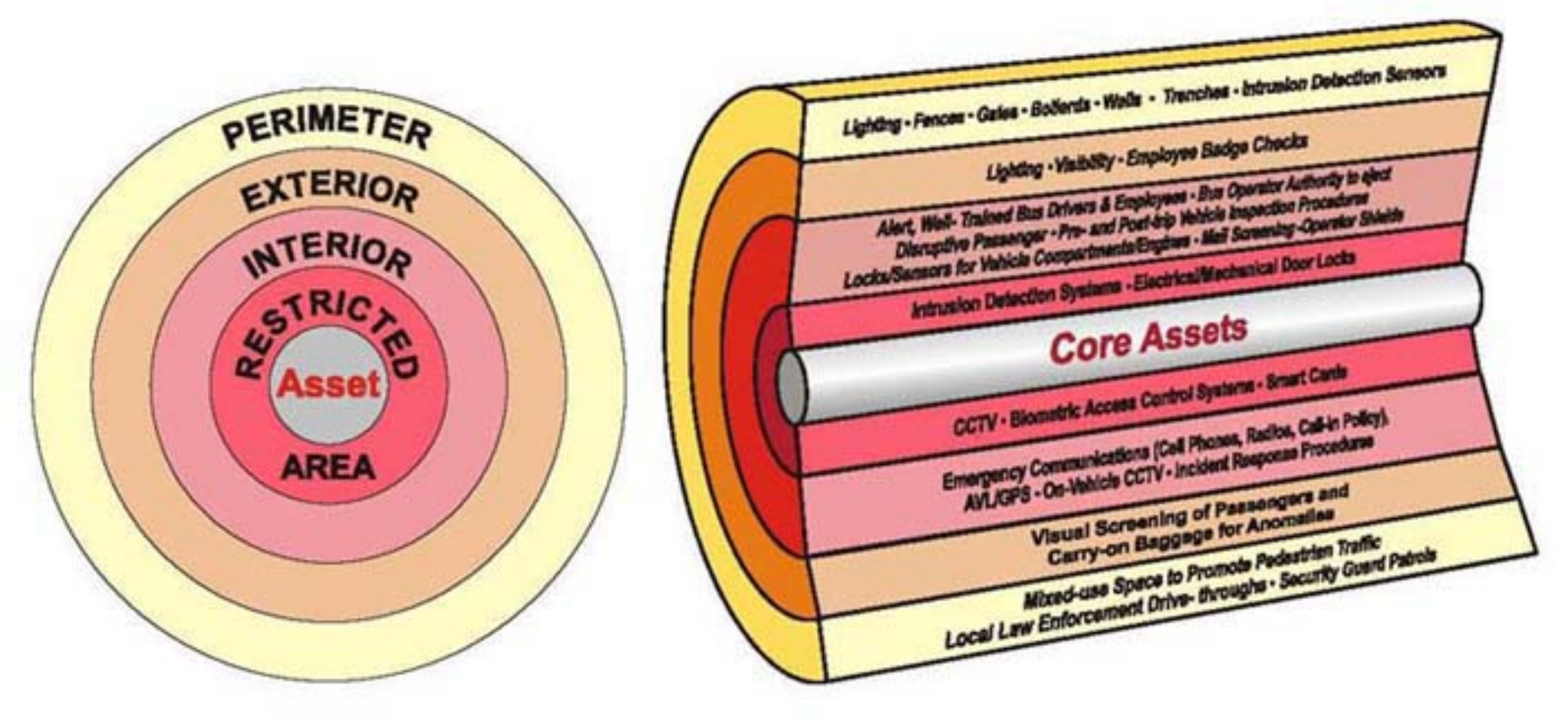
Layers in Clothing



Medieval Layers



Layers in Physical Security


PERIMETER
EXTERIOR
INTERIOR
RESTRICTED
Asset
AREA
Lighting - Fences - Gates - Bollards - Walls - Trenches - Intrusion Detection Sensors
Lighting - Visibility - Employee Badge Checks
Alert, Well- Trained Bus Drivers & Employees - Bus Operator Authority to eject
Disruptive Passenger - Pre- and Post-trip Vehicle Inspection Procedures
Locks/Sensors for Vehicle Compartments/Engines - Mail Screening -Operator Shields
Intrusion Detection Systems - Electrical/Mechanical Door Locks
Core Assets
CCTV - Biometric Access Control Systems - Smart Cards
Emergency Communications (Cell Phones, Radios, Call-in Policy).
AVL/GPS - On-Vehicle CCTV - Incident Response Procedures
Visual Screening of Passengers and
Carry-on Baggage for Anomalies
Mixed-use Space to Promote Pedestrian Traffic
Local Law Enforcement Drive- throughs - Security Guard Patrols

Layers: a start

Security: Mentality & Granularity

- Hiring Replaceable ~~Parts~~People
- Security folks are paranoid: always thinking attack vectors
- JVM Security Manager: too granular
- Intending Consequences:
  getting it right by default

PaaS is Different

Protecting users from other users

PaaS Differences

- User code needs some access
- Multitenant
- Usage: Metering/Logging/Throttling

Share with Care

- Shared services subject to attack
- Attempt read-only & write-only HTTP services
  - Write-Only: Logging
  - Read-Only: Shared "master data"
  - Write-Only: Alerting services
- Careful attachment to shared services
- Forbid Cross-LAN Traffic

Applying Philosophy

- Use proven tools:
  - Network isolation
  - Linux/lxc/Docker
  - Squid
- Understandable isolation model
- Managed with scripts

Wrap Up

- Machines ⇒ Virtualization ⇒ Containers
- Network Isolation 'cause TCP/IP just works
- A layer in the security model

Questions?
Thanks!

- Images copyright their respective creators.
- Image sources:
- http://framework.latimes.com/2012/08/22/tungurahua-volcano-erupts-in-ecuador/#/0
- http://becuo.com/scared-dog-face
- https://catmacros.wordpress.com/2009/10/11/out-damned-spot/
- http://healthfavo.com/labeled-skin-diagrams.html
- http://www.outdoorgearlab.com/a/11061/Introduction-to-Layered-Clothing-Systems
- http://blog.questionmark.com/hard-and-soft-defences-in-our-castle-in-the-cloud
- http://transit-safety.volpe.dot.gov/security/securityinitiatives/designconsiderations/CD/sec5.htm
- http://rugbyfix.com/the-rugby-scrum/
- http://pixshark.com/brick-wall.htm