

# CAN WE TRUST THE ZERO IN ZERO TRUST?

Thomas Fricke  
WHY2025  
August 12, 2025



# HI!



## Thomas Fricke

- Statistical and Quantum Physics
- Linux since 0.91
- System Automation
- DevOps
- Cloud Security Architect
- Digital Sovereignty
  - [openCode](#)
  - [openDesk](#)
  - [Sovereign Tech Fund](#)
- K8S since September 2015





**TRUST VS ZERO TRUST**

**No Checks Needed**

**VS**

**Check Always**



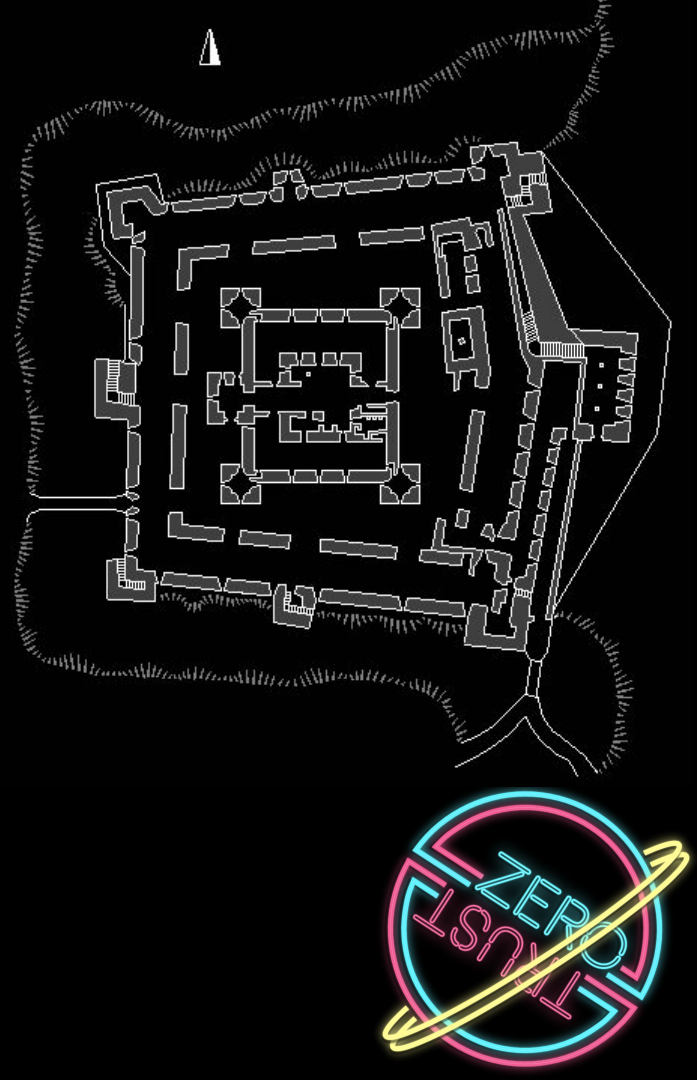
# PERIMETER

Inside: Trust

Outside: No Trust

the principle of concentric design used at Belvoir Castle was to influence castle design for the next several centuries

- One Moat
- Two Walls
- Towers
- Bridges for Access
- surrendered after 18 months





Creative Commons — Attribution-ShareAlike 3.0 Unported — CC BY-SA 3.0

Source: National Maritime Museum of London, Greenwich, photo: Χαράλαμπος Γκούβας ( Harrygouvass)

# WHOM DO YOU TRUST AT THE BORDER?

## Obvious

- One Moat
- Two Walls
- Towers
- Bridges for Access
- Surrendered after 18 months

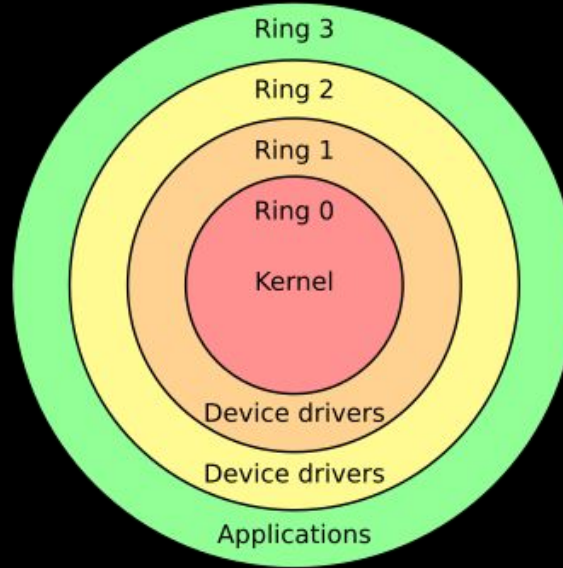
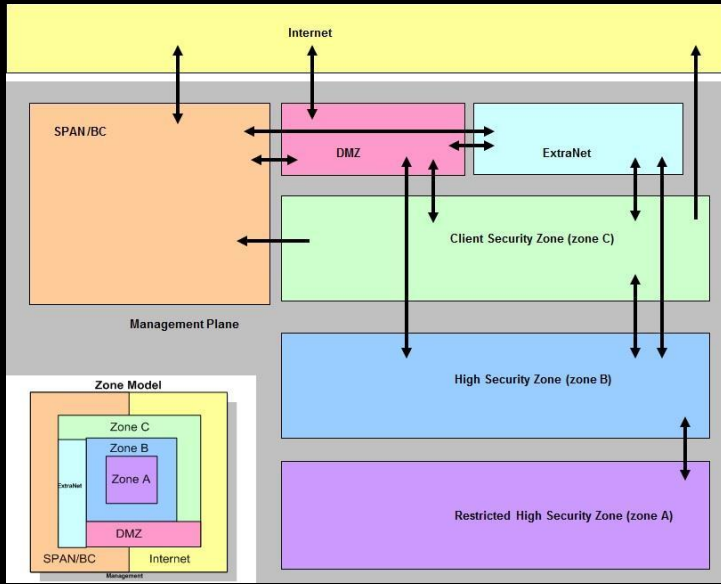
## Implicit

- Bridge
- Doors
- Guards
- Drawbridge mechanics
- Enough stock

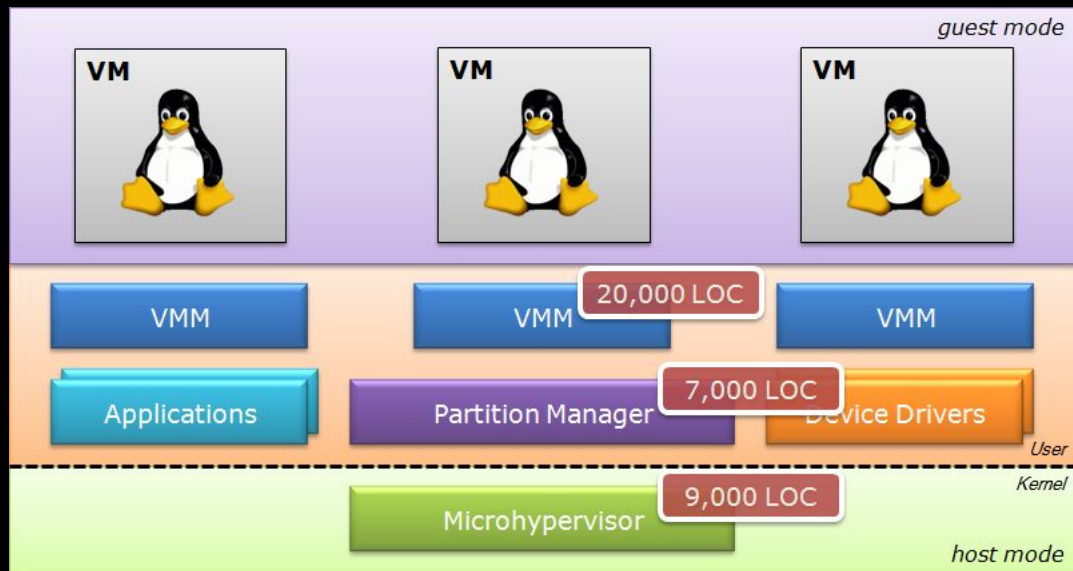


# PERIMETER DESIGN IN IT

- Firewalls: Local Network vs Internet
  - CPU Rings in x86 Architecture
  - Operating System: Privileged Root vs User Mode
- Firewall Software and Settings
  - CPU Microcode and Hypervisor
  - Kernel



# Example: Microkernel



- Trusted Computing Base in [Design and Verification of Secure Systems](#)
- [NOVA Microhypervisor](#)
- Trusted Computing Base is small
- 9000 Lines of Code
- Periphery also small
  - Partition Manager
  - Virtual Machine Manager
- Proven version using the [Rocq Proof Assistant](#)



# SECURITY: THE CORRUPT GUARD PROBLEM

## Problems at the border trusted vs untrusted Zones

- Hidden backdoors in Firewalls
- Hypervisor Breakouts
- Kernel Drivers
- Attestation Processes
- Embargo Processes
- Firmware Update Processes
- ...



## PERIMETER SECURITY BREAK DOWN

- Zero Trust **Network Access**
- How it started
- You have intruders in your network
- Bring your own device
- Hacked
- Internal attacker



# SOLUTIONS AND PROBLEMS

## Solutions

- Ssh
- mTLS (mutual Transport Layer Security)
- VPN

## Problems

- Keymanagment
- Life Cycle
- Host Keys
- Certification Authority Chain
- Point to Point
- Initial key exchange



# ZERO TRUST

If there is so much implicitly trusted stuff we don't trust anybody. Never.

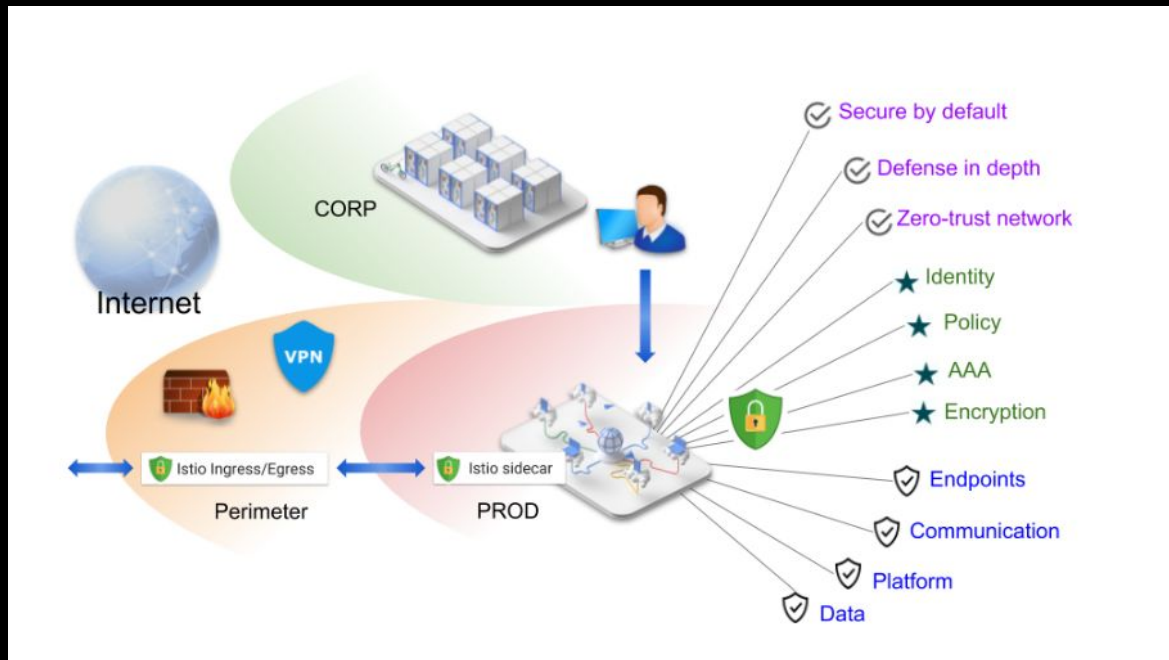
Let's switch to paranoid mode

“Just because you're paranoid doesn't mean they aren't after you.”

— Joseph Heller, *Catch-22*



# ISTIO 1.2



This is all marketing

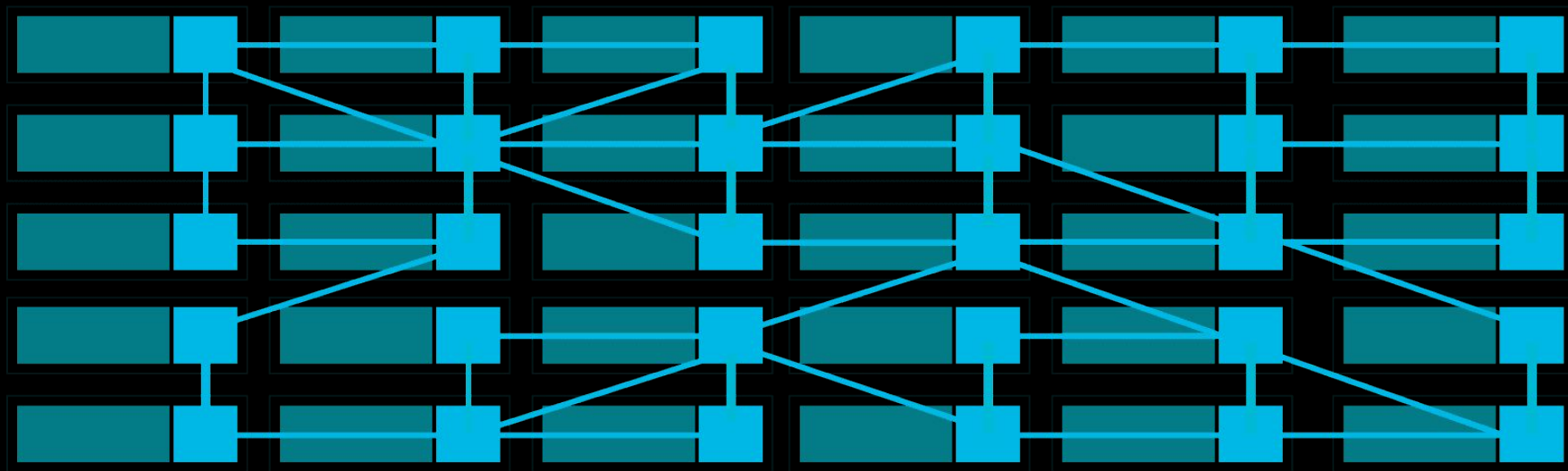
- Zero Trust (Network Access)
- Certification Authority
  - Citadel
  - attached to a HSM
- Sidecars
  - Privileged Containers
  - Envoy
  - Same Network Namespace as Payload
- Has been fixed (somehow™)

BTW: hacked by the speaker

<https://github.com/thomasfricke/training-kubernetes-security/blob/main/IstioHack.ipynb>



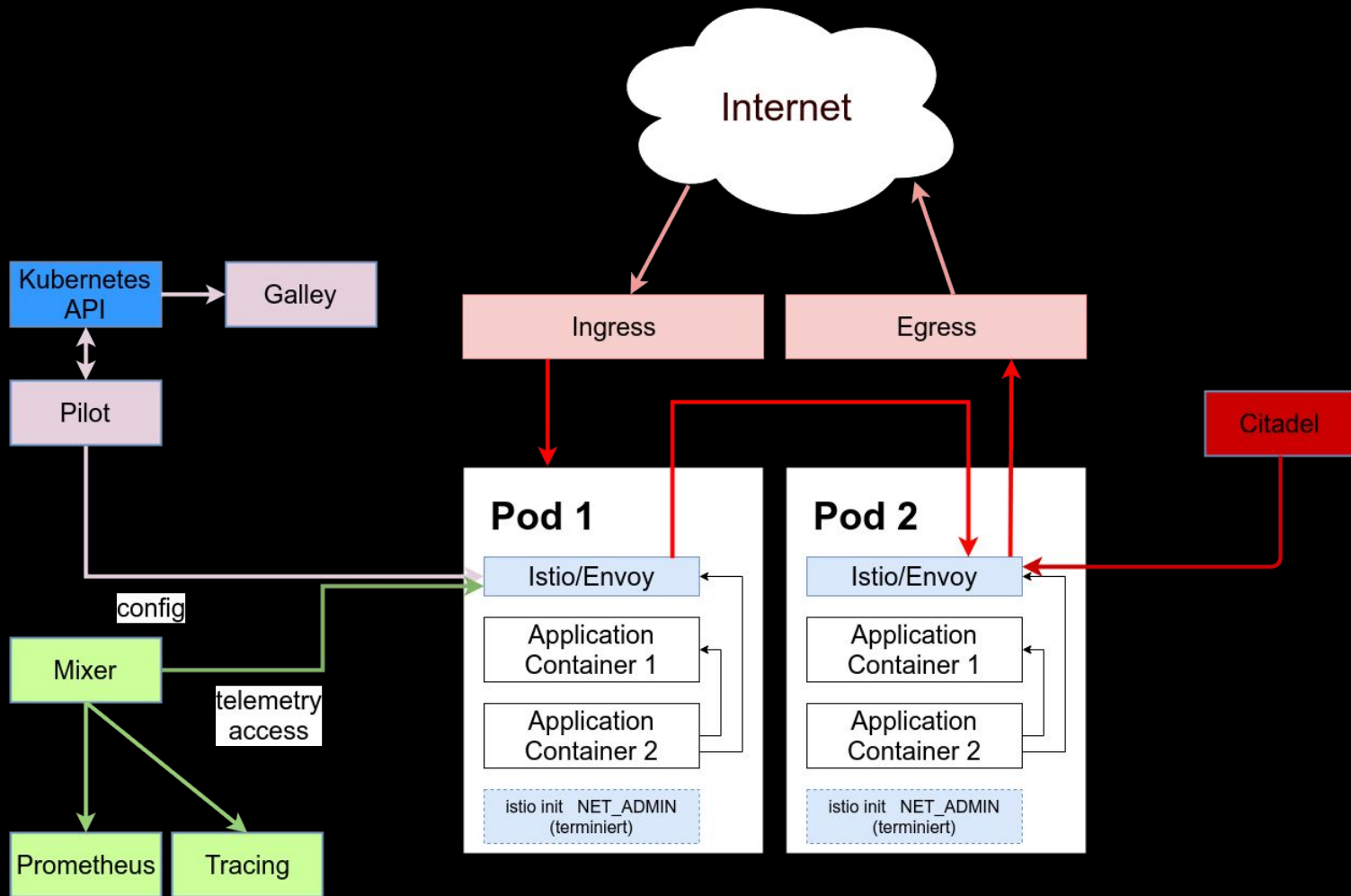
# SERVICE MESH



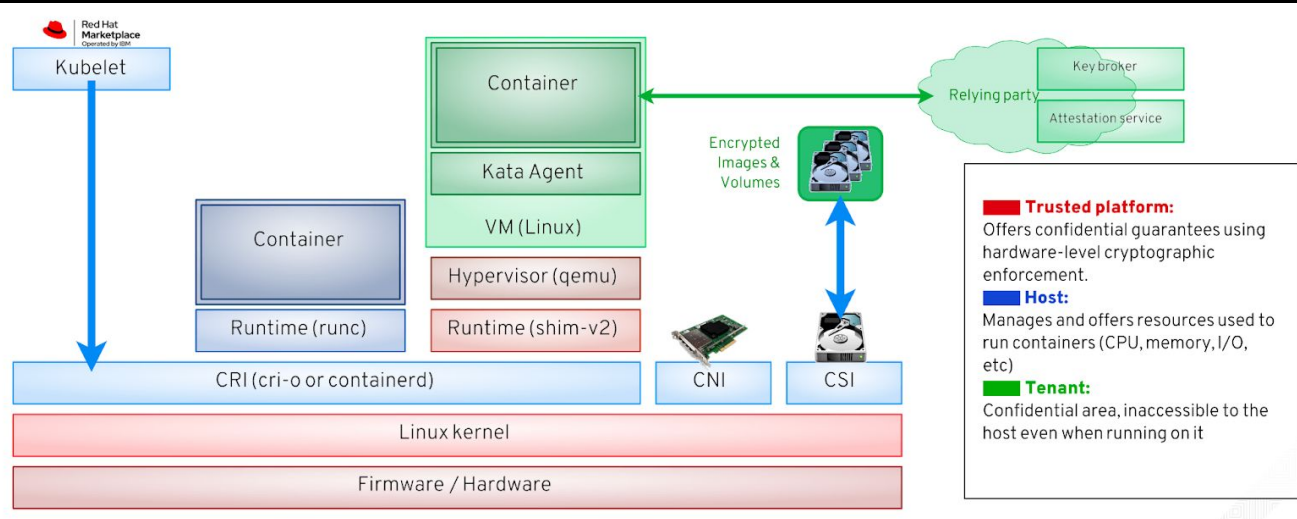
Microservice

Sidecar





# CONFIDENTIAL COMPUTING



## Zero Trust to the Host Owner

- Encryption on Transport (TLS)
- Encryption on Rest (luks+tang)
- Encryption in Memory
- All Future Intel (TDX/SGX) and AMD (SEV) CPUs
- Great 🍌🍌🍌🍌🍌

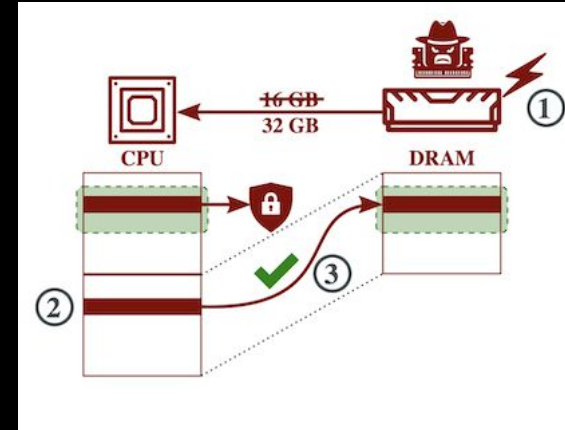


# IMPLICITE TRUST

- **Firmware**
  - Buggy
  - Lot of Legacy Code which cannot be trusted
- **Firmware Updates**
  - Slow
  - 6 months + in the cloud
- **Embargo Process**
  - Trust in nobody is abusing the exploit before fix
  - at first you get a number
  - you have to check
- **Attestation**
  - SGX
  - SGX has been hacked

Rolled out in Health Care

Hacked by [Luca Wilke](#) 10€ Raspi



# ADMINISTRATION

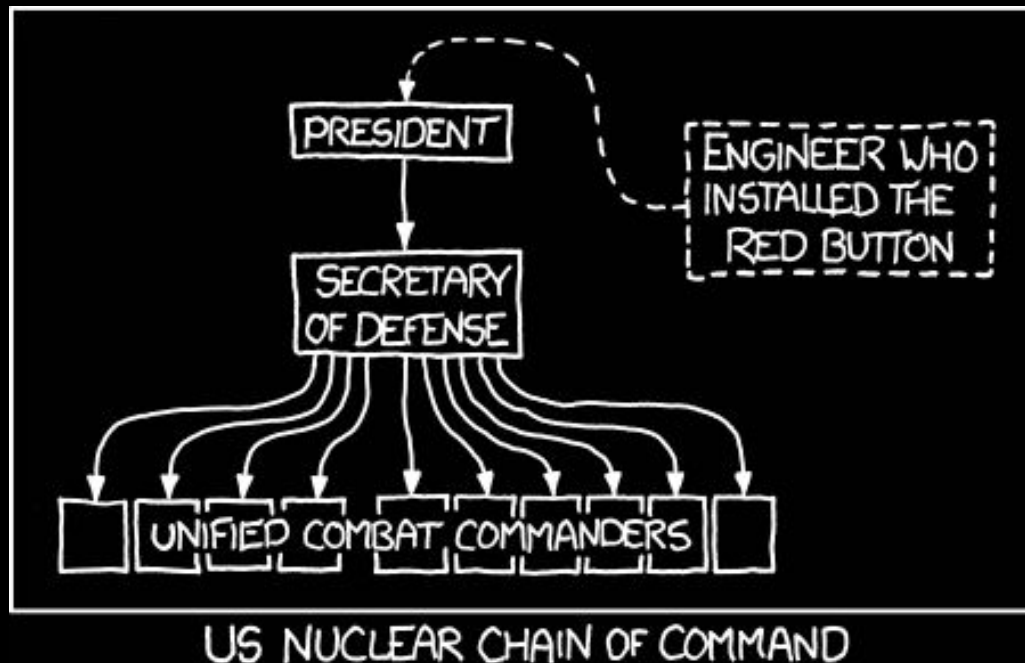
- **Confidential Computing**
- **allows separation of admin roles**
  - **Confidential Operators**
  - **Standard System Operator**
  - **You need to do it**
  - **You need to run the attestation Hardware**
    - **Not in the the cloud**
    - **In your rooms**
- **Otherwise a waste of time**



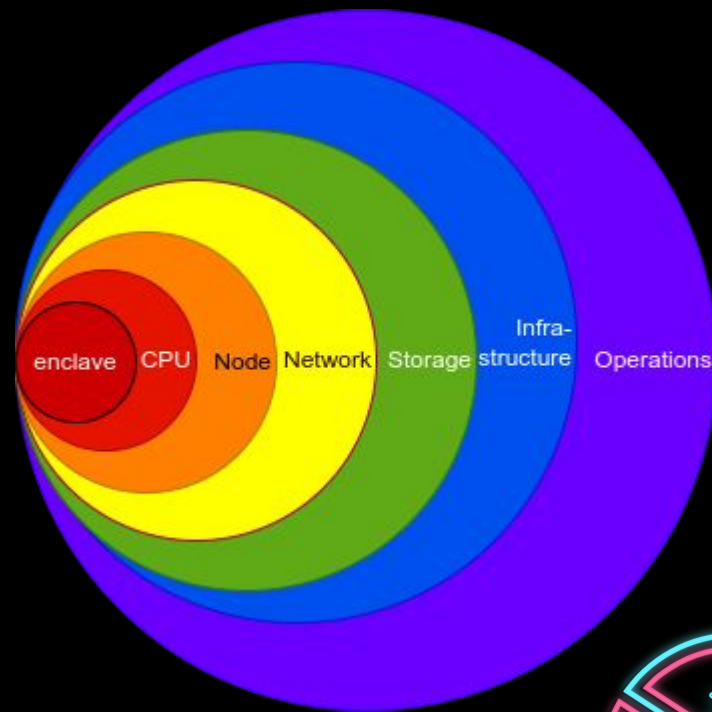
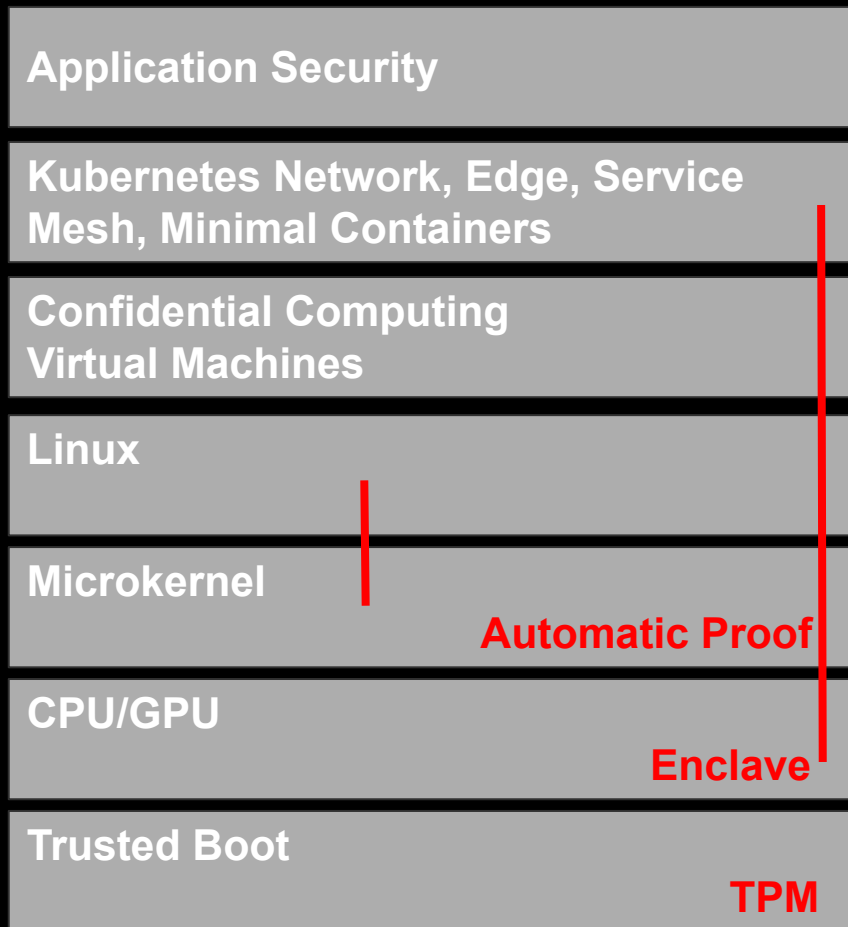
# HIDDEN CONTROL PLANES

What is the Main Control Plane?

- Git
  - Argo CD
  - Kubernetes
- Software Defined Network
- Storage
- Identity and Access Management
- Operations
- ???



# SECURE STACK



# CONCLUSION

“Just because you're paranoid doesn't mean they aren't after you.”

— Joseph Heller, *Catch-22*

- Zero Trust is good for you
- BUT you need to understand it
- Implicite Dependencies
- Implement it correctly
- Avoid overselling



# CONTACT?

<https://thomasfricke.de>

[why2025@thomasfricke.de](mailto:why2025@thomasfricke.de)

<https://23.social/@thomasfricke>

<https://www.linkedin.com/in/thomas-fricke-9840a21/>

