RSAConference2017
San Francisco | February 13 – 17 | Moscone Center

POWER OF OPPORTUNITY

SESSION ID: CSV-T10

What is needed in the Next Generation Cloud trusted platform?

David B. Cross
Director of Cloud Security
Google
@MrDBCross

How Do You Trust a Cloud Platform?

Fact:
Everyone is moving to the cloud

Trust through transparency: Logging, auditing, compliance

Automation: Abstraction, detection and remediation

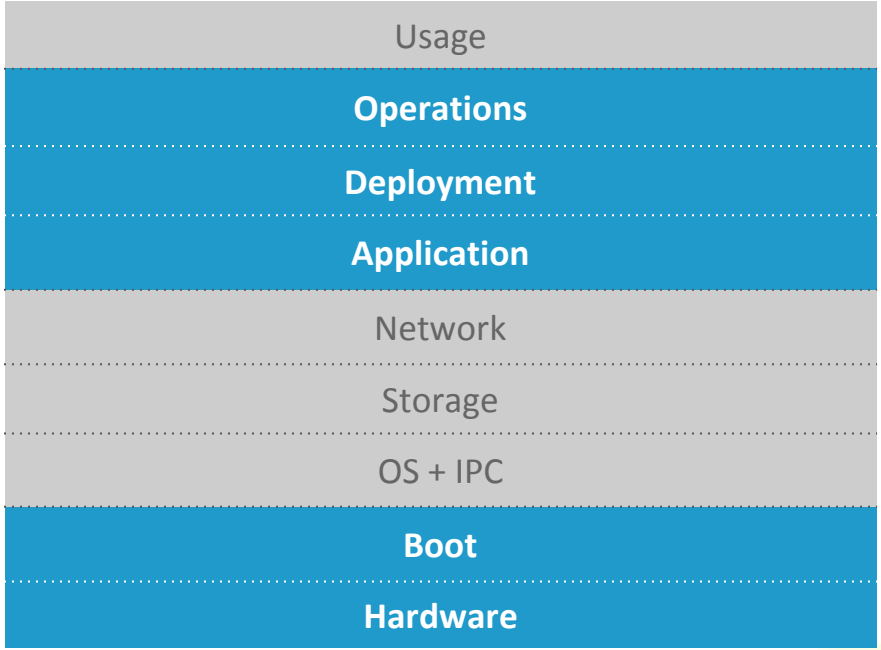
Control: Policy, IAM, encryption, 2FA, etc.

Defense in Depth: Protection at cloud scale via trusted stack

Innovation: Next generation application model

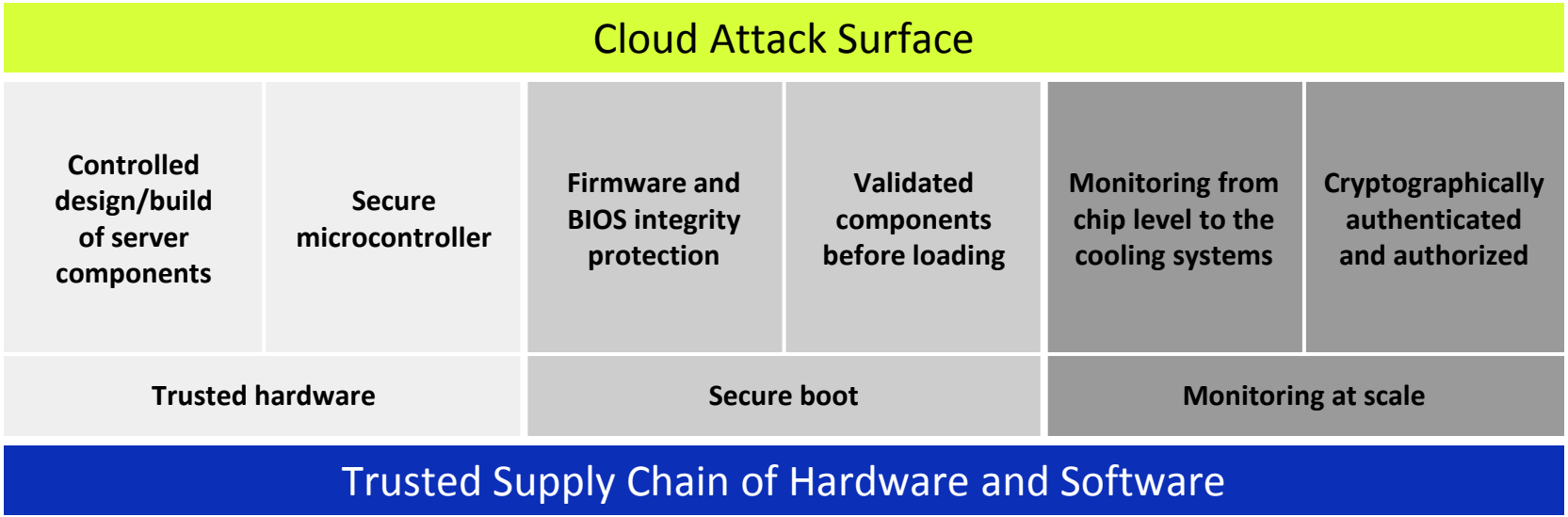
What Comprises a Cloud Trusted Platform?

- Think of the cloud platform as a 9 layer stack
  - From Hardware -> Users
  - Each layer is a security layer
  - Trust is built by ensuring you have security in each layer



Hardware Layer

The Need for a Trusted Hardware Stack



Boot Layer

OS Layer: The Risks Without a Hardened Kernel

Reality: VMs should always be viewed as untrusted

VM Containment is Mission Critical

- Boundary between the host kernel and untrusted code running in a VM
- A separate userspace virtual machine monitor

OS Layer: The Risks of Unknown Hardware

Unknown hardware configurations

The more untrusted software, the risk is exponential

Attack is easier through drivers at the OS layer

Controlled Harware Configurations

Homogeneous system configurations

No legacy hardware or unused devices in cloud datacenter

Tightly controlled software driver supply chain

OS Layer: Recommended Risk Mitigations

- Continuous attack surface reduction. Trim the kernel and hardare drivers to only what is needed
- Constant fuzzing of all components. Attackers do the same.
- Extensive kernel address space randomization and code flow integrity
- All kernel and user mode crashed should be monitored and analyzed. This is how you find the zero days.

RSAConference2017

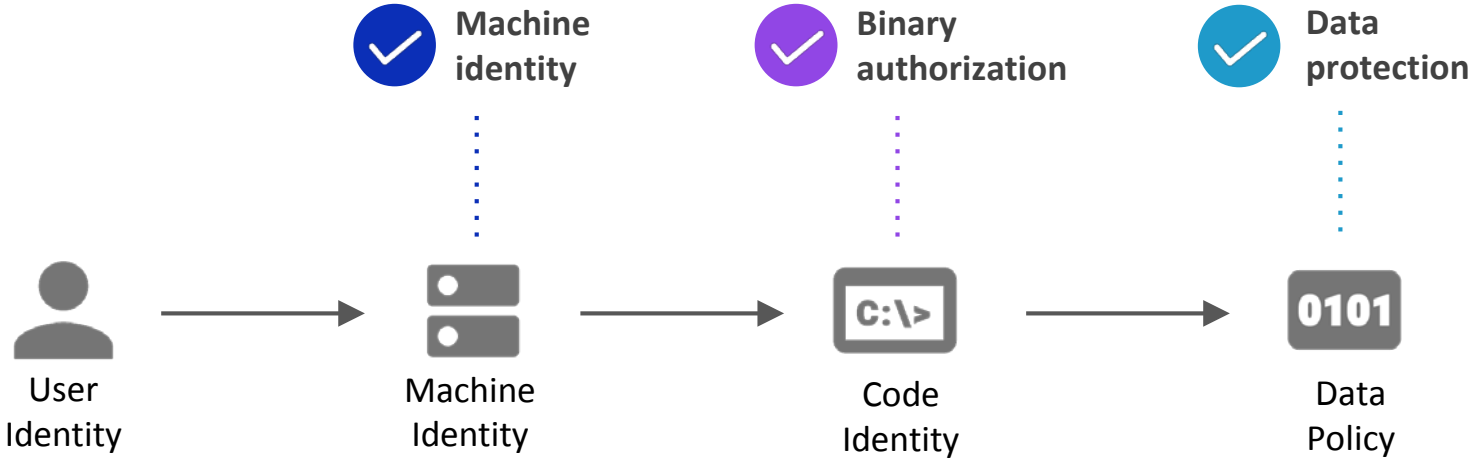
Application Layer

The Cloud Fabric Layer is Evolving

- **Standard Cloud Fabric Definition:** "The loosely coupled storage, networking and parallel processing functions linked by high bandwidth interconnects"

- **Trusted Fabric:** All functions and flows are known and validated through policies and monitoring

Application Layer: Code Has an Identity



- Right code running on the right machine authorized by the right identity accessing the right data at the right time

Trusted Fabric Recommendations

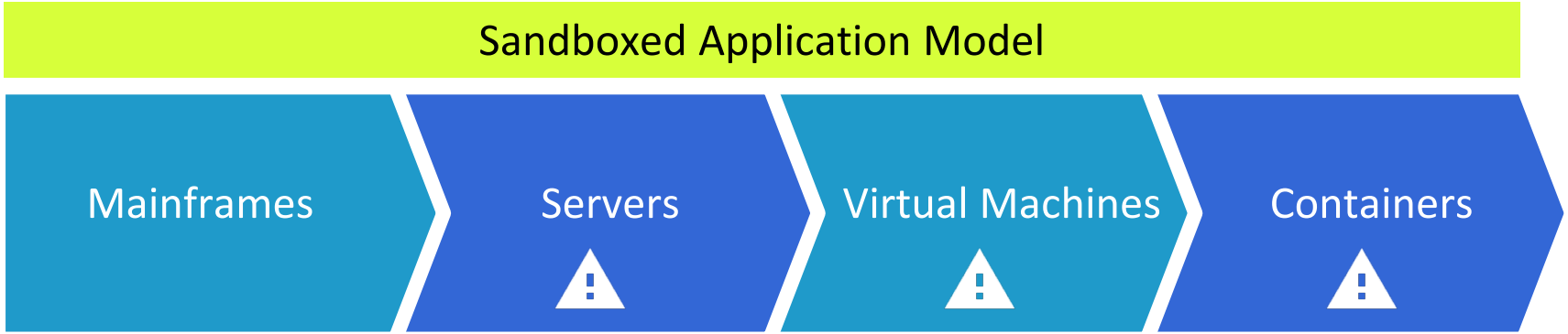
- Code is always tested and reviewed
- Only execute code with known cryptographic signatures and trusted provenance
- All jobs and policy changes audited automatically
- Code and machine identity tightly bound by policy
- Compartmentalization of code based on its role

Despite this Evolution We are Not Secure

Multi-tenant systems do not have adequate partitioning of resources

The container security ecosystem and isolation is still immature

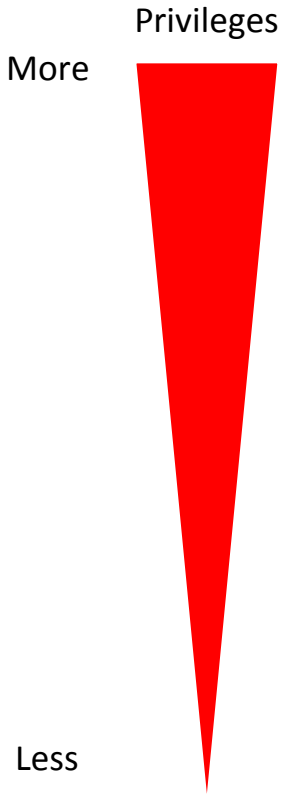
Consider a Sandboxed Application Model



Host kernel syscall are the continued source of big risk

Sandboxing the application environment reduces this risk

Sandboxed Applications – The Challenges



Untrusted app

		On Premise Datacenter	Cloud
Compute	Privileged instruction isolation	Supervisor bit, SMEP	VMs, Containers
Memory	Privileged memory isolation	ASLR, SMAP, TrustZone	Cloud Storage
OS/IO/Disk	Machine resource isolation	chroot, namespaces, capabilities	GCP, AWS
User Data	User data isolation	File permissions, encryption	IAM, Encryption at rest, user supplied keys

Sandboxed Applications - Philosophy

Defense Layers

- Independent security boundaries
- Combining diverse technologies in single sandbox
- No single vulnerability affects all user data

Sandboxed Applications - Philosophy

Maintenance

- Continuous internal and external reviews
- Assume attackers have all your source code
- Unit, functional and fuzz testing
- Continuous integration and deployment of upstream changes

Sandboxed Applications - Philosophy

Monitoring

- Logging at all layers, all the time
- Central repository and tamper resistance
- Alerting and incident response processes
- Incidents are how you improve the system

The Continued Application Layer Risks

Problem:

We all have secrets!

Protecting secrets is increasingly hard

- Database credentials
- Passwords
- API and OAuth tokens
- SSH keys
- SSL certs and keys, etc…
- IP protected algorithms

The Next Generation Cloud Application Model

The Past

Past Ecosystem Solutions Explored:

TPMs were the "hope" for trusted applications

Intel TXT and AMD SVM (secure hypervisor launch) also had potential...

The Next Generation Cloud Application Model

Looking forward into the future:

Secure Isolated Execution Environments (SIEEs)

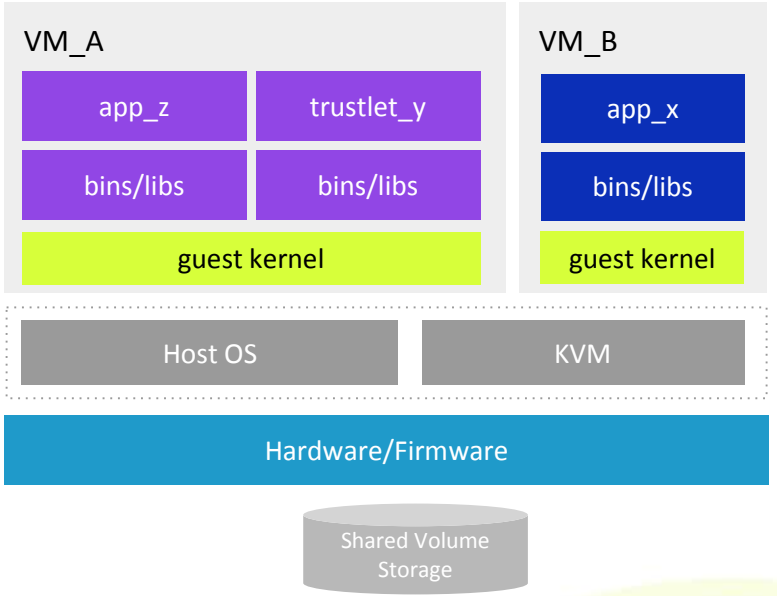
The Potential Solution:

Software enclaves with attestation and optional hardware

Next Generation Cloud Apps Using Hardware

The benefits of hardware

- Reduce the Trusted Computing Base to the smallest footprint
- Protect memory against bus snooping and memory tampering attacks
- Protect against root-level admins and malicious users
- Attested and verified



The Next Generation Cloud Application Model

Emerging industry technologies:

Intel SGX hardware enclaves

- Dedicated HW chip as a root-of-trust
- Hardware-assisted isolation of code execution
- Fully attested state (pre-OS, Host OS, VM, and Enclaves)
- Verifiable by consumers

AMD Secure Encrypted Virtualization

- Encrypted guest memory
- Restricted key access

RSAConference2017

Deployment Layer

Deployment: Strong Multi-Factor Authentication

- The boundaries are down and the model is changing
- 2FA and security keys are here now
- Session re-use and lack of device binding is the continued risk
- Advance MFA usage with other policy constraints

Secret Protection is Critical

Token Reuse	Strong Authentication
Hardware session binding and enforcement	Policy based, unphishable authentication using Security Key

RSAConference2017

Operations Layer

Ops Layer: Machine Learning is Not the Only Answer

Two motions must be combined at the ops layer to achieve Defense in Depth:

1. Environment specific endpoint policies
2. Machine learning analysis

Trusted Machine + Trusted Person + Untrusted Location + Untrusted Time = **High Risk**

Apply: Best Practices when Moving to the Cloud

1

Examine
the cloud platform security stack in detail from an end to end hardware and software perspective

2

Establish
end to end trust capabilities and policies from devices to your data

3

Explore
building next generation applications to be to be sandboxed and using hardware isolation

4

Ensure
your cloud security policies use both your environment policies with machine learning analysis