Designing a Secure Cloud

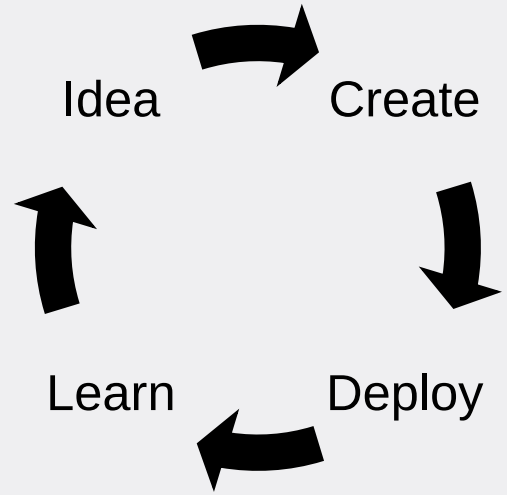
Cloud@MICRO 2021

Hybrid Cloud Infrastructure
IBM Research

Paul G Crumley pgc@us.ibm.com
Robert Senger rmsenger@us.ibm.com
Seetharami “Seelam” sseelam@us.ibm.com
Ming-Hung Chen minghungchen@ibm.com
Jaime H Moreno jhmoreno@us.ibm.com

Cloud Data Centers are evolving quickly, fueled by business needs

Cloud infrastructure and processes can increase business velocity



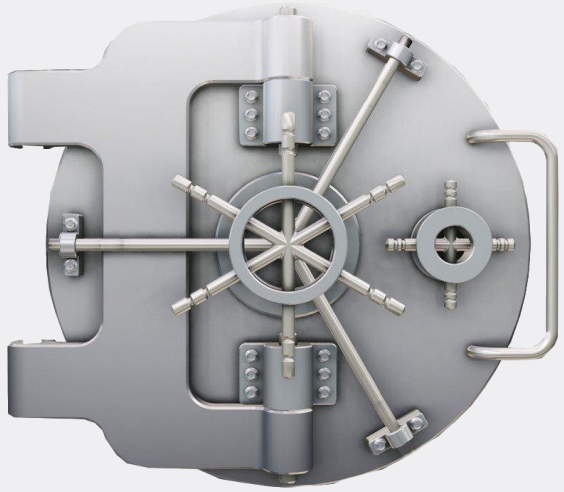
Infrastructure is consumed using **APIs** to integrate with DevOps and to enable automation

When there are few constraints, **ideas can evolve quickly**

- Many ideas do not survive to experience “enterprise” issues

Requirements I hear from enterprise clients for cloud infrastructure

Enterprises desire the benefits of cloud
but have demanding requirements



Security: Integrity, Isolation, Business Continuity

Compliance: Validation, Immutable Logs, Reporting

Risk / Cost: Reducing risk can be more significant than financial cost

Examples of enterprise requirements conflicting with legacy designs in cloud

Firmware is used to implement critical aspects of security and data functions

- Where does this firmware come from? Who validates it?
- Blindly installing new FW / SW can get one fired ☹

Proliferation of interfaces for (remote) control

- Many ad-hoc & legacy solutions. **Far too much "magic"**
- Clients must be isolated from the configuration and management functions

Mechanisms to debug and validate systems in situ

- Signal injection of test data and errors is done to validate error detection and correction
- These allow any memory, register, or signal to be interrogated

Some devices **claim** isolation

- Our tests have penetrated some of the security barriers
- We need provably correct devices and secure interface protocols

Two Challenges

How do enterprise clients **trust** cloud infrastructure?

- They must be able to examine the hardware, firmware, and software
- Must know the configuration of resources being used
- Mechanisms enforce configurations and capture data for verification

How to **securely** provide **flexibility and efficiency**?

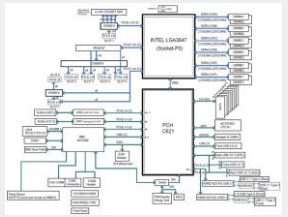
- Traditional techniques often bring problems
- No “Magic Permitted”
- Tension between security and programmatic configurability

What work needs to be done now to meet these challenges?

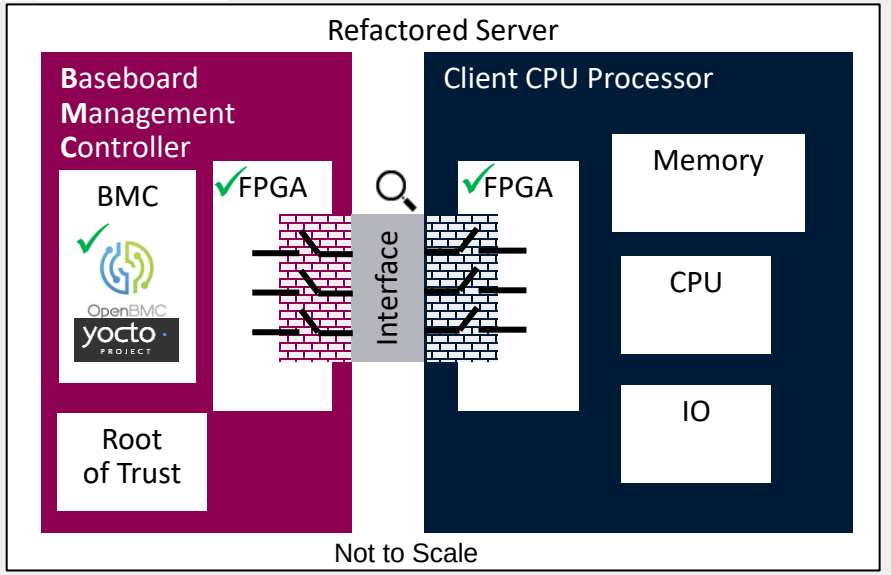
- Are there designs and interfaces which should be deprecated now to prepare?

A Current Research Project: Isolation & Trust using DC-SCM & OpenBMC

Problem: How do clients trust the infrastructure?



*



DC-SCM: (Data Center – Secure Control Module)

- Separate management and client boards with defined interface
- Any interactions across boundary are observed and logged
- Clients have hardware isolation from administrators
- Administrators have hardware isolation from clients
- Client board can be stateless to eliminate temporal attack "surfaces"

OpenBMC: (Baseboard Management Controller)

- Community provides an open implementation of the management code running in the BMC board
- Clients can inspect code and map source code to signatures
- Clients can verify ✓ the signature of code which impacts resources a client is using
- Unneeded BMC code can be removed to reduce attack surfaces and bugs
- Specialized BMC and CPU code can be loaded, when needed, for debug / validation purposes

Relative Scale

*Supermicro X11SPA T Block Diagram

Some Longer-Term Research Work: Secure Resource Composability

Secure composability is already a capability in enterprise systems

- The are “partitioned”, not “shared”

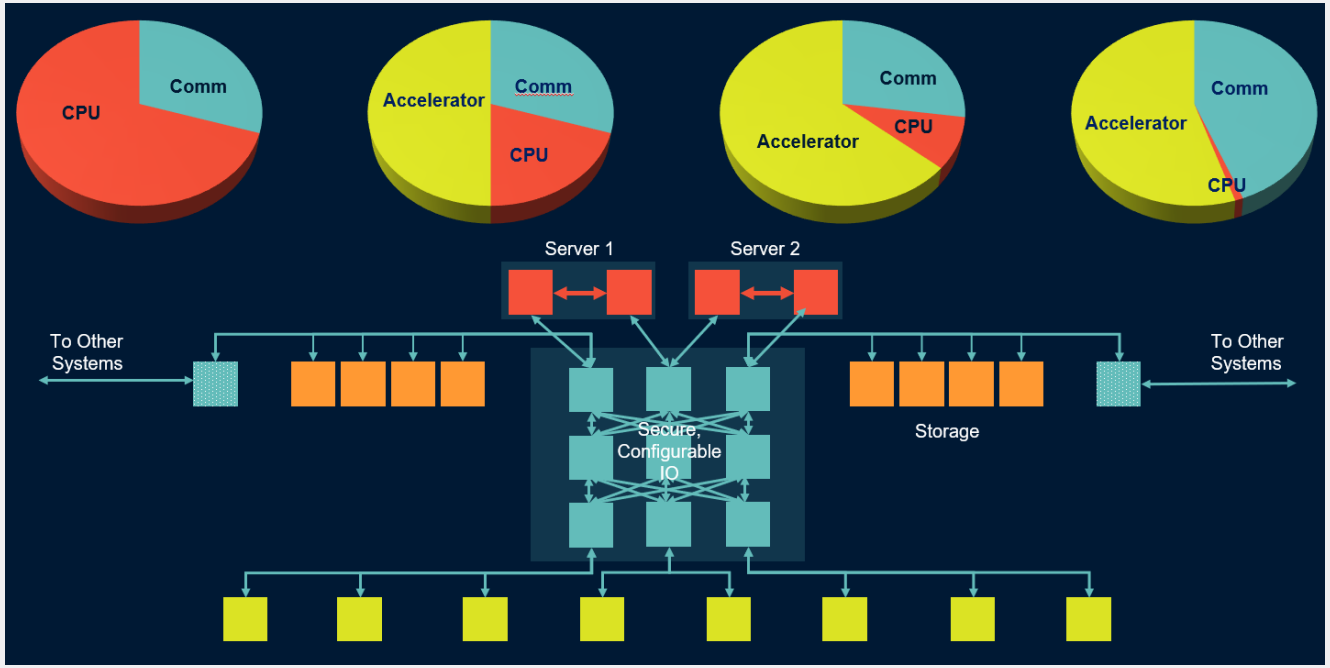
Secure Composability allows resources to be tailored to workload

- Used to provide security, performance, and legacy support

Working with technology communities to develop the base technologies

- Open Compute Project
- CXL / PCI-SIG / Open Fabrics

Our research team is investigating secure composition capabilities for a broader set of workloads at larger scale



Additional Areas for Exploration

Architecture for secure, multi-tenant cloud

- Current architectures and system components are designed for a different time and place
- How to securely and efficiently map cloud abstractions and processes to infrastructure
- Is sharing over-rated?

Secure mechanisms for telemetry, validation, and debug

- How can infrastructure provide debug/configuration capabilities without compromising security?

Tools & Processes to validate designs and ensure supply chain security

- Design and verification for security requirements from the start
- How do we know the boards and modules precisely match the specifications?

What attack surfaces can we eliminate?

- Don’t spend effort hardening problem spots that can be removed
- Every component must be essential to keep verification cost manageable and reduce risk
- Paul’s personal goal is to remove all persistent firmware storage from infrastructure

Summary

Opportunities to expand cloud adoption by addressing challenges of

- **Security**: Integrity, Isolation, Robustness
- **Efficiency**: Secure and flexible configuration of resources

Next steps: Call to action

- Many other topics to allow us to securely tailor infrastructure for cloud
- What must be done **now** to clear a path to better security in cloud infrastructure
- Help us grow the community with more academic ideas and projects

Thank you for your time and attention

Notices and disclaimers

U.S. Government Users Restricted Rights — use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM.

Information in these presentations (including information relating to products that have not yet been announced by IBM) has been reviewed for accuracy as of the date of initial publication and could include unintentional technical or typographical errors. IBM shall have no responsibility to update this information. **This document is distributed "as is" without any warranty, either express or implied. In no event shall IBM be liable for any damage arising from the use of this information, including but not limited to, loss of data, business interruption, loss of profit or loss of opportunity.** IBM products and services are warranted according to the terms and conditions of the agreements under which they are provided.

IBM products are manufactured from new parts or new and used parts.
In some cases, a product may not be new and may have been previously installed. Regardless, our warranty terms apply."

Any statements regarding IBM's future direction, intent or product plans are subject to change or withdrawal without notice.

Performance data contained herein was generally obtained in a controlled, isolated environments. Customer examples are presented
as illustrations of how those customers have used IBM products and the results they may have achieved. Actual performance, cost, savings or other results in other operating environments may vary.

References in this document to IBM products, programs, or services does not imply that IBM intends to make such products, programs or services available in all countries in which IBM operates or does business.

Workshops, sessions and associated materials may have been prepared by independent session speakers, and do not necessarily reflect the
views of IBM. All materials and discussions are provided for informational purposes only, and are neither intended to, nor shall constitute legal or other guidance or advice to any individual participant or their specific situation.

It is the customer's responsibility to insure its own compliance with legal requirements and to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions
the customer may need to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer is in compliance with any law.

Notices and disclaimers continued

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products in connection with this publication and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products. IBM does not warrant the quality of any third-party products, or the ability of any such third-party products to interoperate with IBM's products. **IBM expressly disclaims all warranties, expressed or implied, including but not limited to, the implied warranties of merchantability and fitness for a particular**, **purpose.**

The provision of the information contained herein is not intended to, and does not, grant any right or license under any IBM patents, copyrights, trademarks or other intellectual property right.

IBM, the IBM logo, ibm.com, Aspera®, Bluemix, Blueworks Live, CICS, Clearcase, Cognos®, DOORS®, Emptoris®, Enterprise Document Management System™, FASP®, FileNet®, Global Business Services®, Global Technology Services®, IBM ExperienceOne™, IBM SmartCloud®, IBM Social Business®, Information on Demand, ILOG, Maximo®, MQIntegrator®, MQSeries®, Netcool®, OMEGAMON, OpenPower, PureAnalytics™, PureApplication®, pureCluster™, PureCoverage®, PureData®, PureExperience®, PureFlex®, pureQuery®, pureScale®, PureSystems®, QRadar®, Rational®, Rhapsody®, Smarter Commerce®, SoDA, SPSS, Sterling Commerce®, StoredIQ, Tealeaf®, Tivoli® Trusteer®, Unica®, urban{code}®, Watson, WebSphere®, Worklight®, X-Force® and System z® Z/OS, are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at: www.ibm.com/legal/copytrade.shtml.