Open. Together.

OCP
SUMMIT

HW Management

Manageability Security

James Mihm
BMC FW Architect/Team Lead
Intel Corporation

OPEN PLATINUM™

Todays Snapshot

MANAGEMENT

- Use Redfish For Manageability
- OCP Defined Profiles For Redfish
- OpenBMC Now Supports Redfish
  - Including OCP Profiles
- OpenBMC Security Workgroup
  - Security Architecture Specification
  - Reporting Process
  - Incident Response Team
  - Security Advisory

Motivation

MANAGEMENT

Unified Security Objectives and Requirements for HW & FW

Obligation To Protect & Defend Against Adversaries

- Make It Personal

Ever Increasing Threat Landscape

Goes Beyond DOS or PDOS

- Espionage
- National Security
- Data Protection

Changing Landscape

From Obscurity to Headlines

MANAGEMENT

IPMI: Express Train to Hell, by Dan Farmer published in 2013

http://www.fish2.com/ipmi/itrain-gz.pdf

https://blog.rapid7.com/2013/07/02/a-penetration-testers-guide-to-ipmi/

With a metasploit framework to reference

Bloomberg Article – Hype or Not?

Trammel Hudson’s Project: https://trmm.net/Modchips

CVE-2019-6260 Exploit of AST2400/2500 Bare Metal Recovery Features

Evolution of Thought

MANAGEMENT

Host Interface Implicitly Trusted
- Don’t worry be happy
- Once You Have The Host The Game Is Over

Security Ownership
- Defense in Depth Strategy

Development of Advanced Features
- Ultimate OOB OS Access and Control

Contention Between Usability and Security
- Extremely Secure – Unusable
- Extremely Flexible – Unsecure

Sleepness Nights

MANAGEMENT

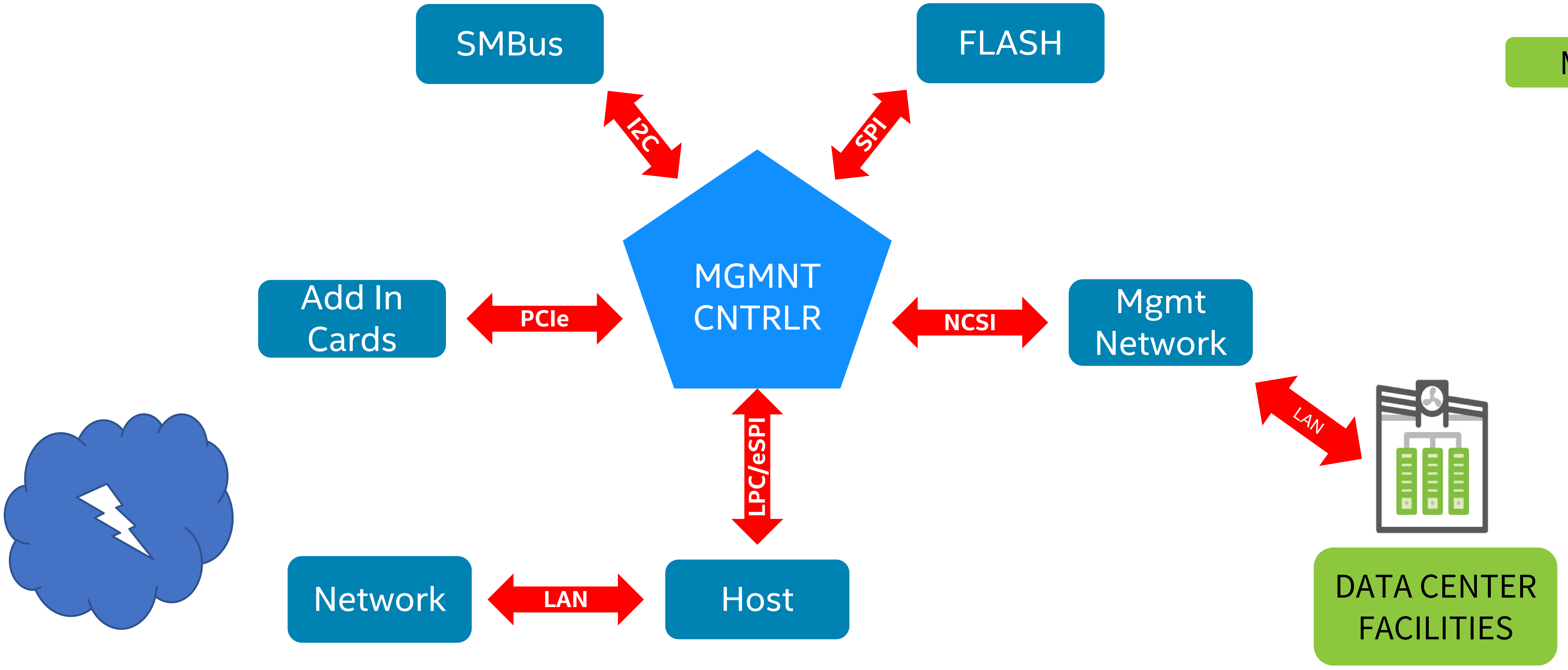
- Insider Threats
  - The Rogue FW Developer
- Nation States
  - Who Can You Trust?
- Supply Chain
  - Measurement, Detection, and Notification
  - Abuse Of Manufacturing Features

Security Recommendations

MANAGEMENT

- Expect More From Vendors
- Definition Of Security Requirements
- Adopt Security Design Lifecycle
  - Learn & Embrace SDL For All Ingredients (HW/SW/FW)
  - Own Your Security
- Architect For Security
  - Avoid Reinventing
  - Provisioning Gate
  - Evaluate Access Controls
  - Hardware Protections

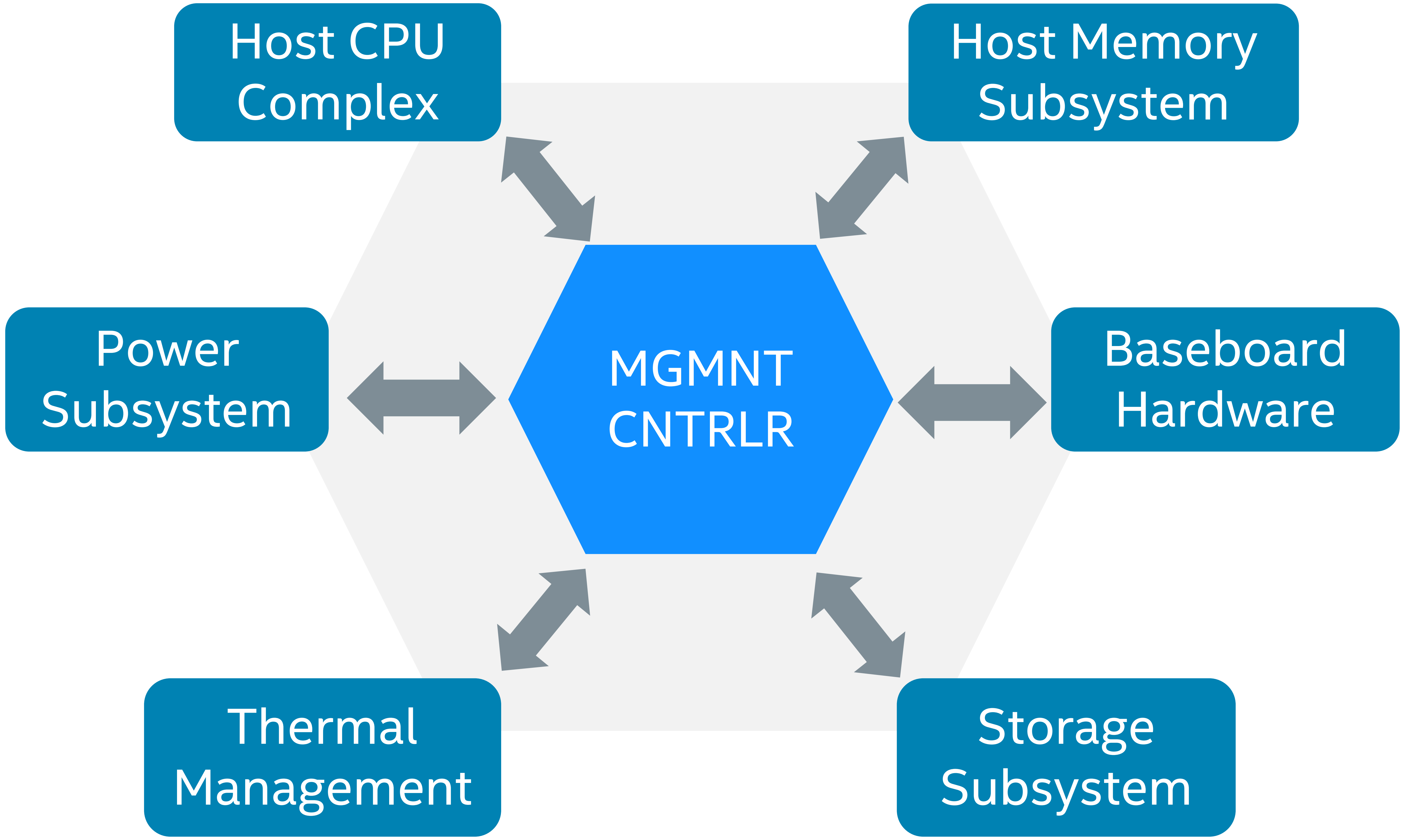
Threat Model – Interfaces



MANAGEMENT

Threat Model – High Value Assets

MANAGEMENT



Call To Action

MANAGEMENT

Define Security Requirement & Architecture Specification

Collaborate on PMCI Security Rqmts (next presentation)

Open Source Firmware Meetup @Marriott Salon V & VI

OpenBMC Security Workgroups

Where to find additional information
OpenBMC Security WG: https://github.com/openbmc/openbmc/wiki/Security-working-group
SDL: https://www.microsoft.com/en-us/securityengineering/sdl/

Open. Together.

OCP Global Summit | March 14–15, 2019

OCP
SUMMIT