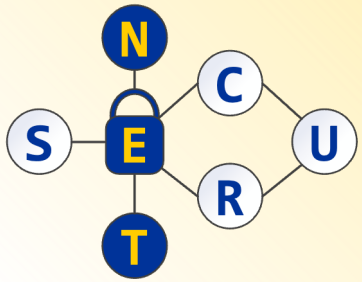


Enhancing Cross-Sectoral Collaboration in Cybersecurity in Estonia, Czechia, Lithuania, Ukraine, and the Netherlands

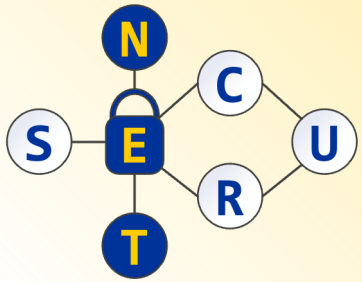
Funded by the European Union

Security Risk Management of Baseboard Management Controller

Raimundas Matulevičius

Professor of Information Security, University of Tartu, Estonia
Lead of the InfoSec Research Group
Coordinator of the SECURE-NET project

Funded by the European Union Horizon Europe programme under Grant Agreement No. 101217315. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.



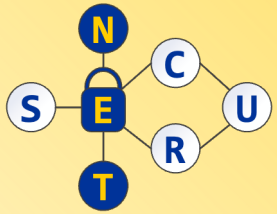
Enhancing Cross-Sectoral Collaboration in Cybersecurity in Estonia, Czechia, Lithuania, Ukraine, and the Netherlands

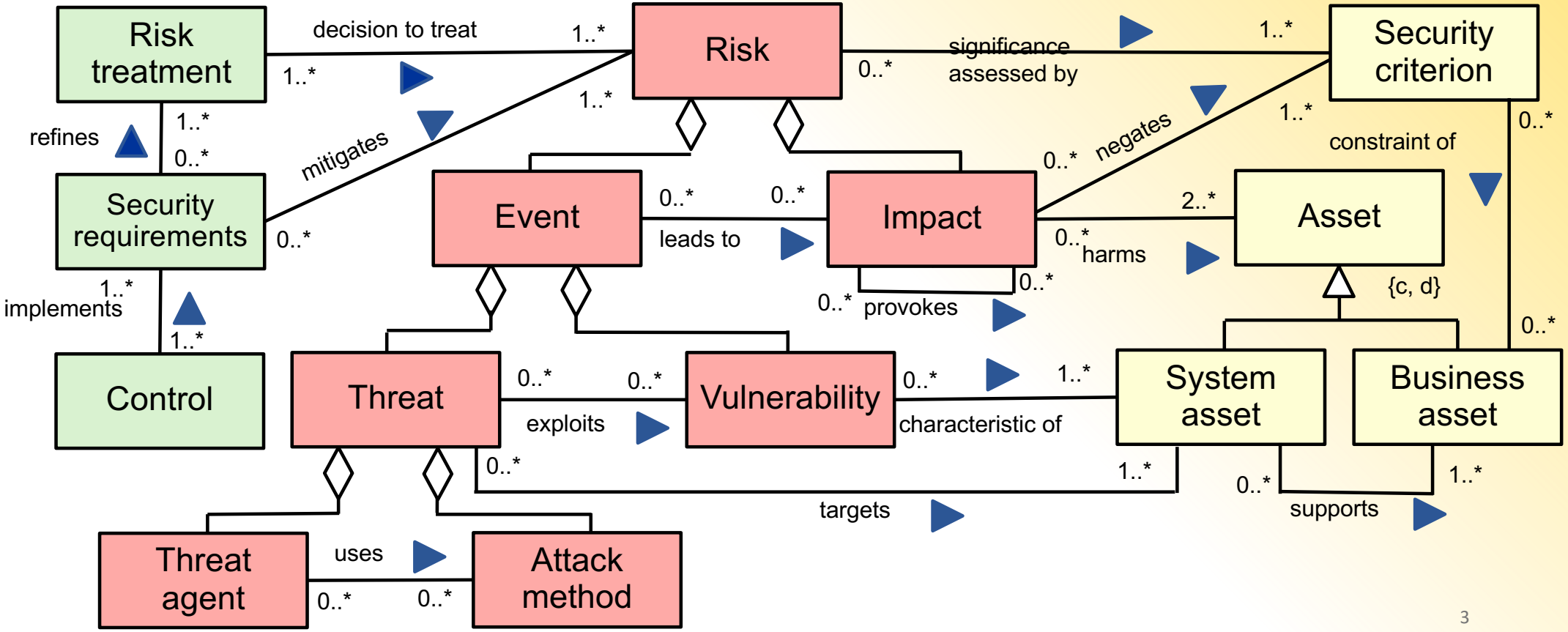
Funded by the European Union

What is Security Risk Management?

Funded by the European Union Horizon Europe programme under Grant Agreement No. 101217315. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

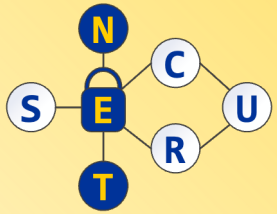
Domain Model for
Security Risk Management





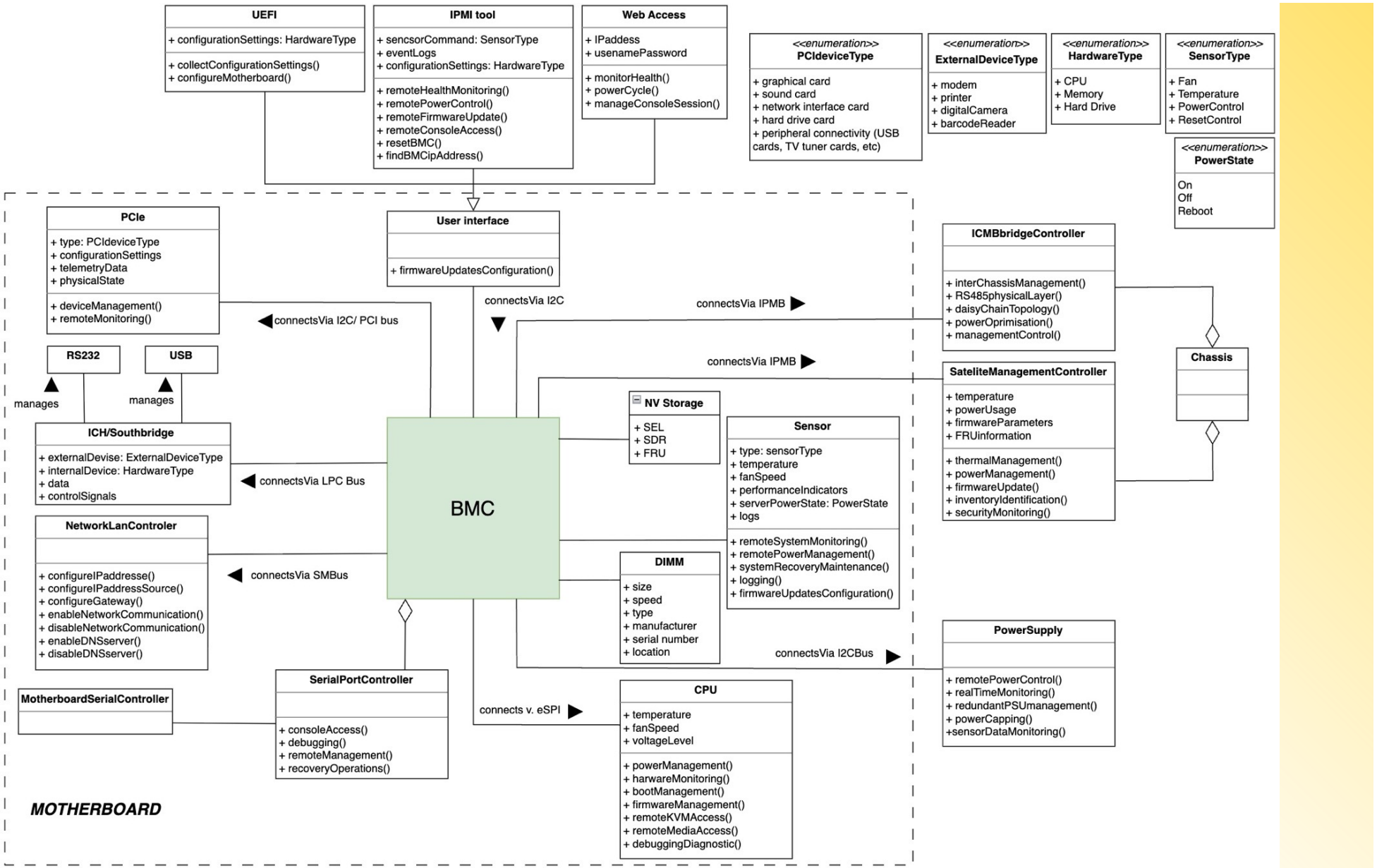
Security Appraisal Framework

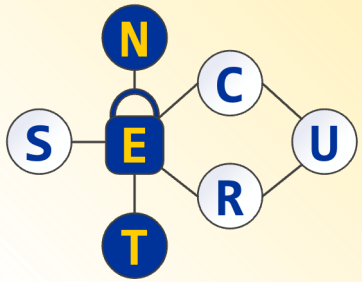
OCP: Open Compute Project



- **Critical Assets**
  - A listing of all security-impacting assets within the firmware, and the corresponding Confidentiality, Integrity and Availability requirements for each
- **Attack Surface Enumeration**
  - A listing of all remote, local and physical attack surfaces exposed by the device
- **Adversarial Model**
  - A listing of all threat actors along with their motivation and capabilities
- **Security Objectives**
  - The high-level security objectives or key risks exposed by the firmware

https://github.com/opencomputeproject/OCP-Security-SAFE/blob/main/Documentation/framework.md


UEFI
+ configurationSettings: HardwareType
+ collectConfigurationSettings()
+ configureMotherboard()
IPMI tool
+ sencsorCommand: SensorType
+ eventLogs
+ configurationSettings: HardwareType
+ remoteHealthMonitoring()
+ remotePowerControl()
+ remoteFirmwareUpdate()
+ remoteConsoleAccess()
+ resetBMC()
+ findBMCipAddress()
Web Access
+ IPaddess
+ usenamePassword
+ monitorHealth()
+ powerCycle()
+ manageConsoleSession()
<<enumeration>>
PCIdeviceType
+ graphical card
+ sound card
+ network interface card
+ hard drive card
+ peripheral connectivity (USB cards, TV tuner cards, etc)
<<enumeration>>
ExternalDeviceType
+ modem
+ printer
+ digitalCamera
+ barcodeReader
<<enumeration>>
HardwareType
+ CPU
+ Memory
+ Hard Drive
<<enumeration>>
SensorType
+ Fan
+ Temperature
+ PowerControl
+ ResetControl
<<enumeration>>
PowerState
On
Off
Reboot
PCIe
+ type: PCIdeviceType
+ configurationSettings
+ telemetryData
+ physicalState
+ deviceManagement()
+ remoteMonitoring()
User interface
+ firmwareUpdatesConfiguration()
ICMBbridgeController
+ interChassisManagement()
+ RS485physicalLayer()
+ daisyChainTopology()
+ powerOprimisation()
+ managementControl()
Chassis
SateliteManagementController
+ temperature
+ powerUsage
+ firmwareParameters
+ FRUinformation
+ thermalManagement()
+ powerManagement()
+ firmwareUpdate()
+ inventoryIdentification()
+ securityMonitoring()
connectsVia I2C/ PCI bus
connectsVia I2C
connectsVia IPMB
connectsVia IPMB
RS232
USB
manages
manages
ICH/Southbridge
+ externalDevise: ExternalDeviceType
+ internalDevice: HardwareType
+ data
+ controlSignals
connectsVia LPC Bus
BMC
NV Storage
+ SEL
+ SDR
+ FRU
Sensor
+ type: sensorType
+ temperature
+ fanSpeed
+ performanceIndicators
+ serverPowerState: PowerState
+ logs
+ remoteSystemMonitoring()
+ remotePowerManagement()
+ systemRecoveryMaintenance()
+ logging()
+ firmwareUpdatesConfiguration()
NetworkLanControler
+ configureIPaddresse()
+ configureIPaddressSource()
+ configureGateway()
+ enableNetworkCommunication()
+ disableNetworkCommunication()
+ enableDNSserver()
+ disableDNSserver()
connectsVia SMBus
DIMM
+ size
+ speed
+ type
+ manufacturer
+ serial number
+ location
PowerSupply
+ remotePowerControl()
+ realTimeMonitoring()
+ redundantPSUmanagement()
+ powerCapping()
+sensorDataMonitoring()
connectsVia I2CBus
SerialPortController
+ consoleAccess()
+ debugging()
+ remoteManagement()
+ recoveryOperations()
MotherboardSerialController
connects v. eSPI
CPU
+ temperature
+ fanSpeed
+ voltageLevel
+ powerManagement()
+ harwareMonitoring()
+ bootManagement()
+ firmwareManagement()
+ remoteKVMAccess()
+ remoteMediaAccess()
+ debuggingDiagnostic()
MOTHERBOARD



Enhancing Cross-Sectoral Collaboration in Cybersecurity in Estonia, Czechia, Lithuania, Ukraine, and the Netherlands

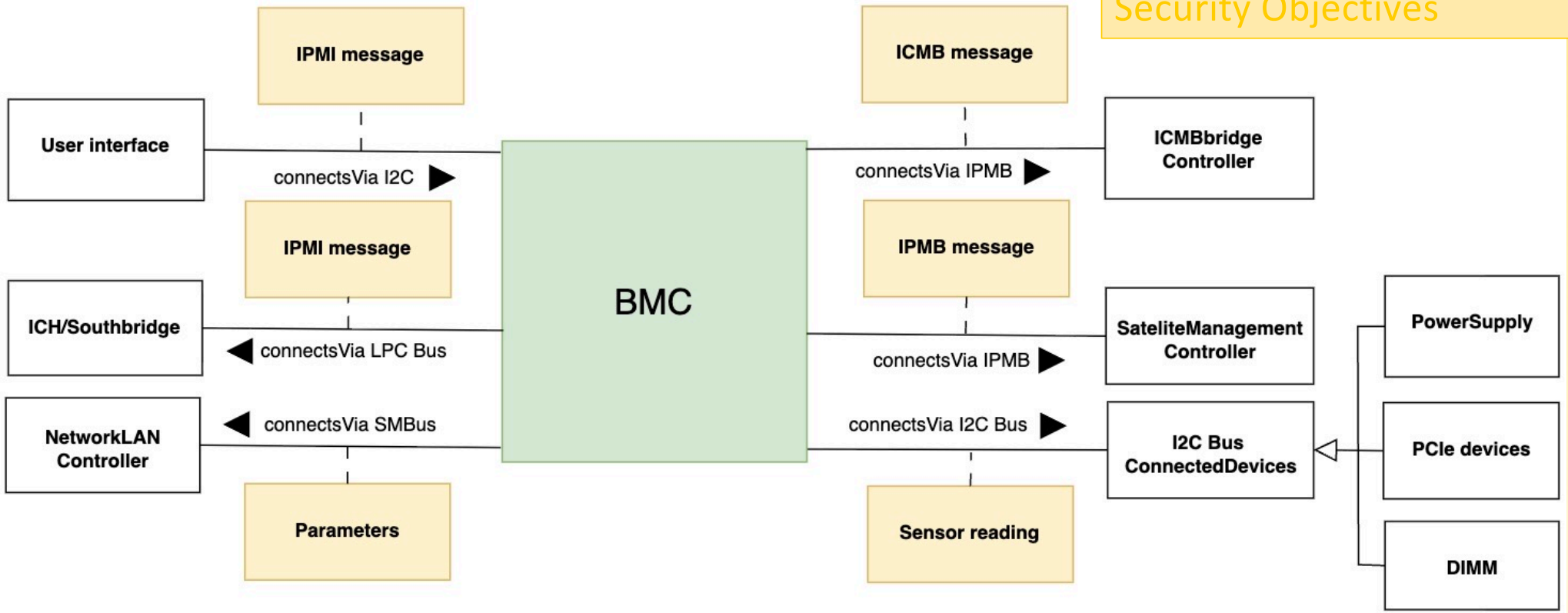
- Critical assets
- Attack Surface Enumeration
- Adversarial model
- Security Objectives

Application of Security Appraisal Framework for BMC

Funded by the European Union Horizon Europe programme under Grant Agreement No. 101217315. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

Critical Assets

- Critical assets
- Attack Surface Enumeration
- Adversarial model
- Security Objectives



"Treating firmware, credentials, and out-of-band channels as primary assets" [LinkedIn comment]

Attack Surface Enumeration

Critical assets

Attack Surface Enumeration

Adversarial model

Security Objectives

Capture: How does the system capture data? How is data entered into the system?

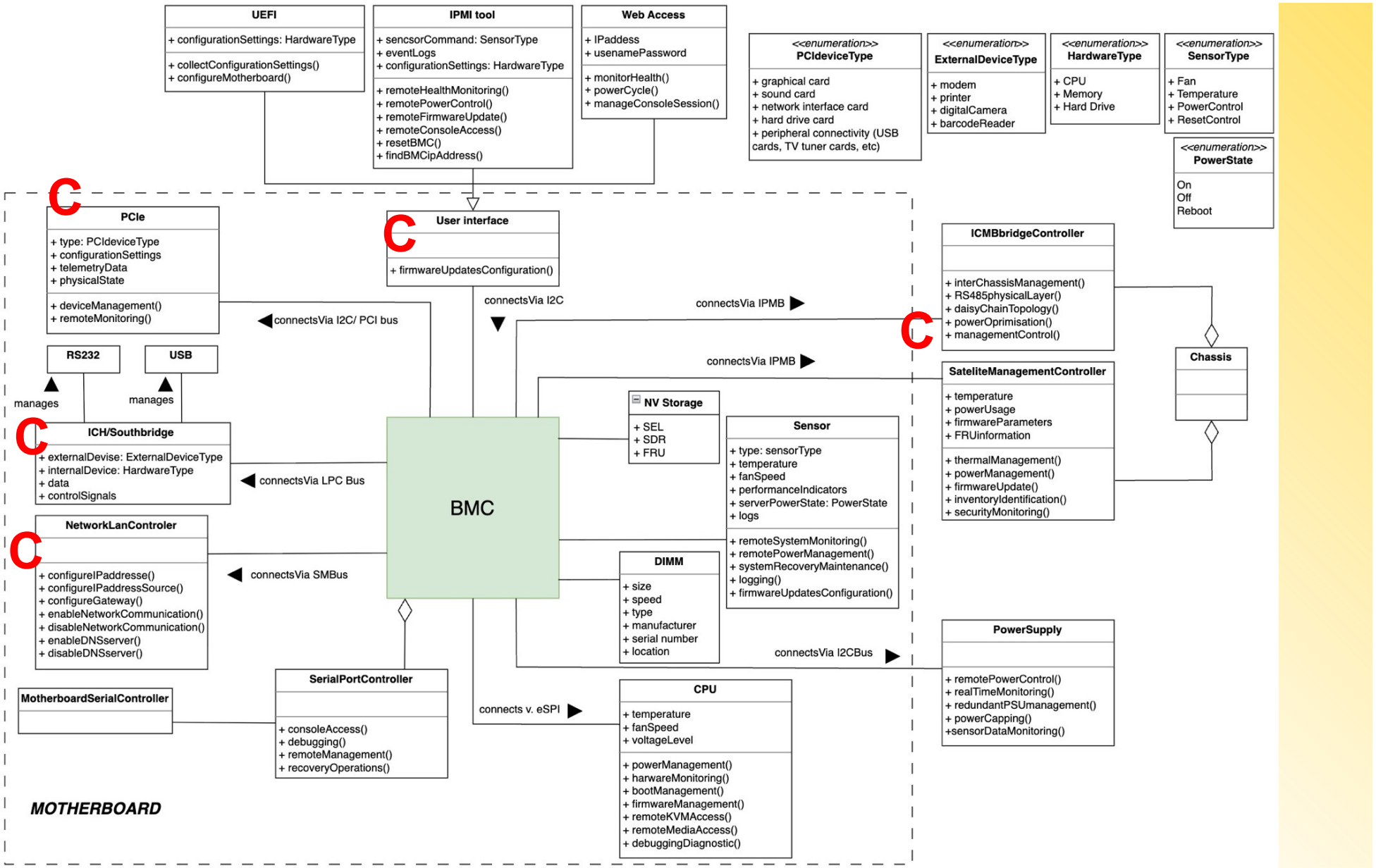
Transmit: How is data transmitted between different devices?

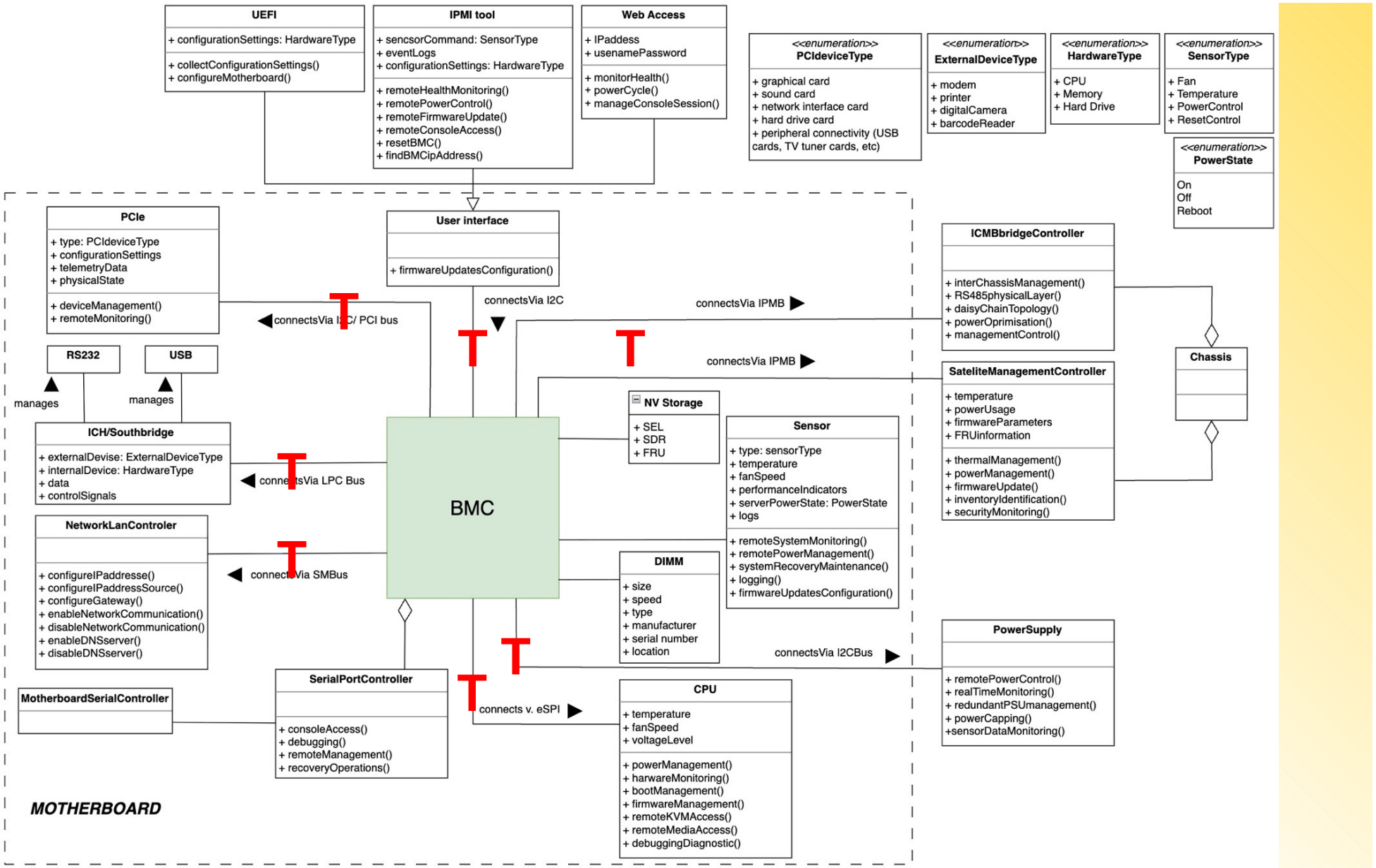
Store: How is data stored in the device (format, type, structure of storing, etc)?

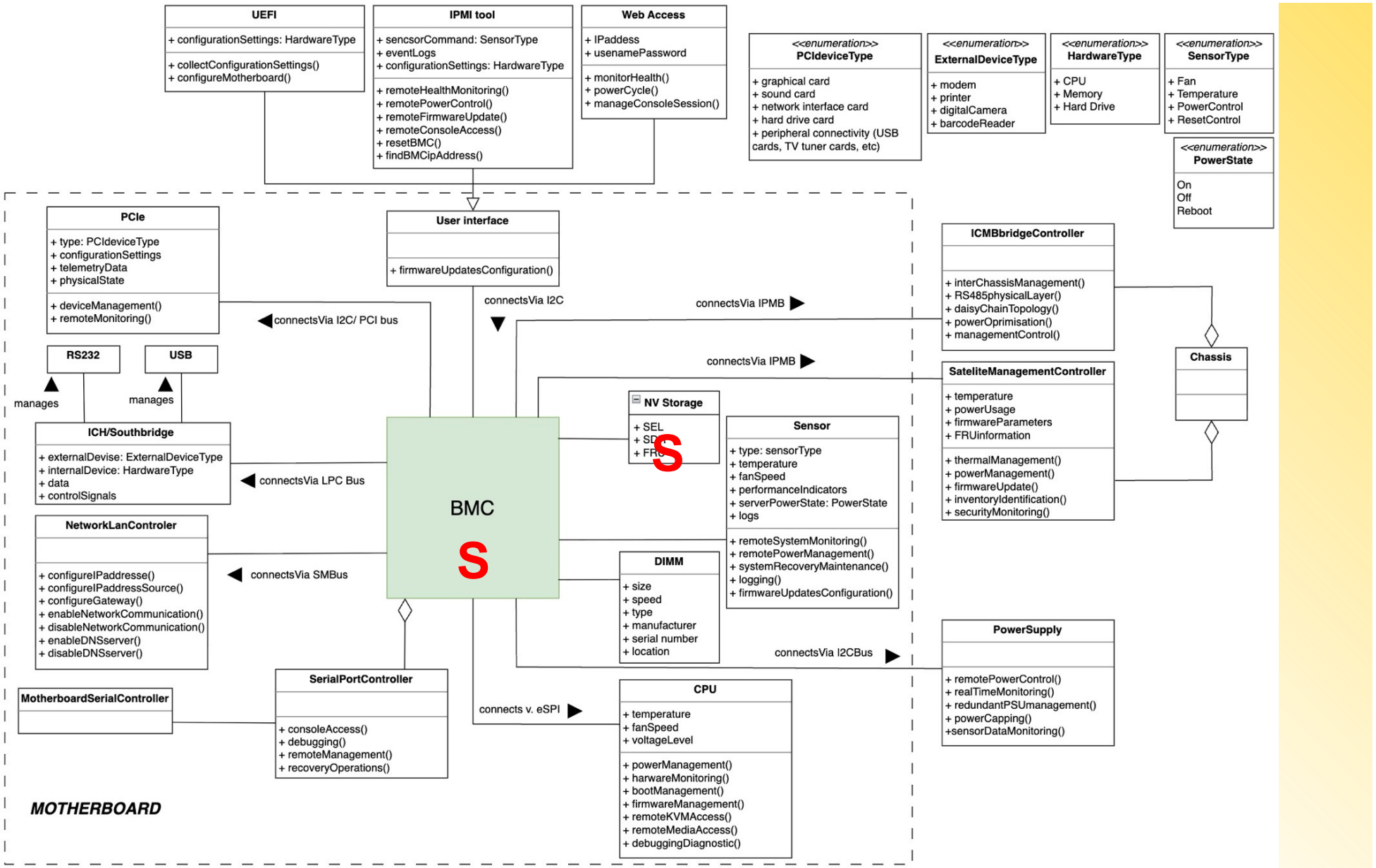
Retrieve: How isdata are retrieved from the device (permissions)?

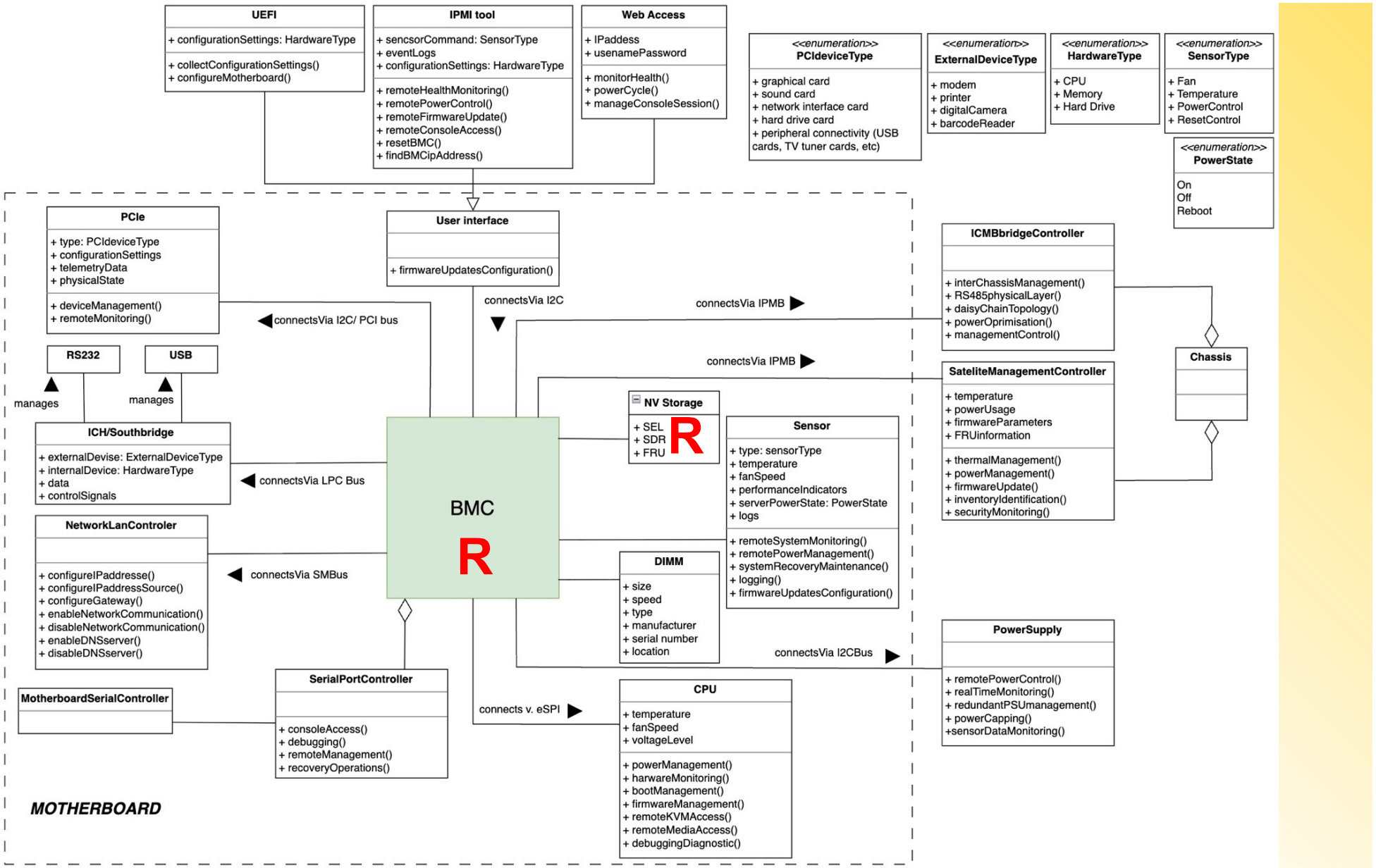
Manipulate: How is data calculated, compared, estimated, changed, aggregated, etc?

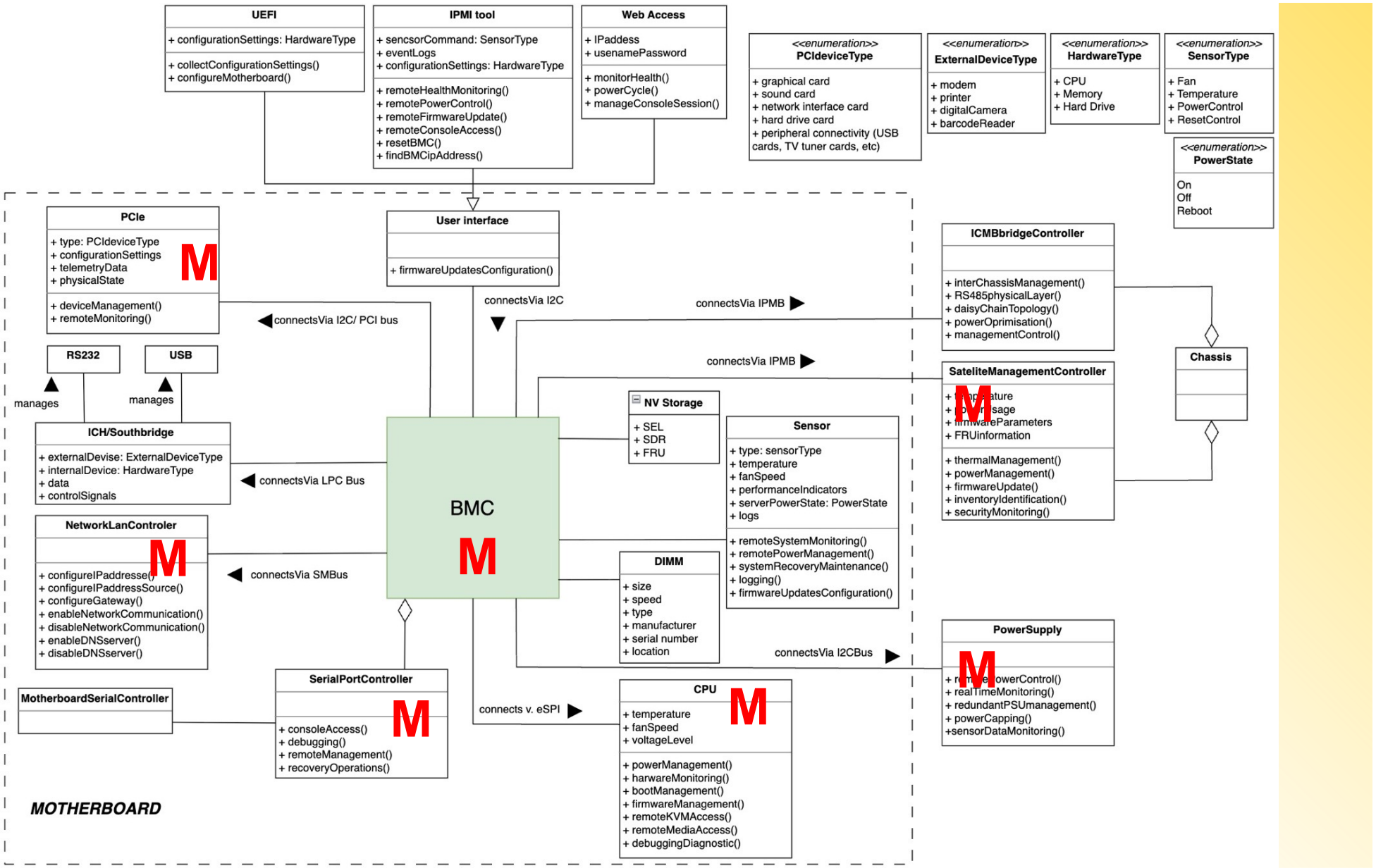
Display: How data is displayed to the user/ administrator (correctness of display, authorised access to see the displayed data, use of the received/ displayed data)?

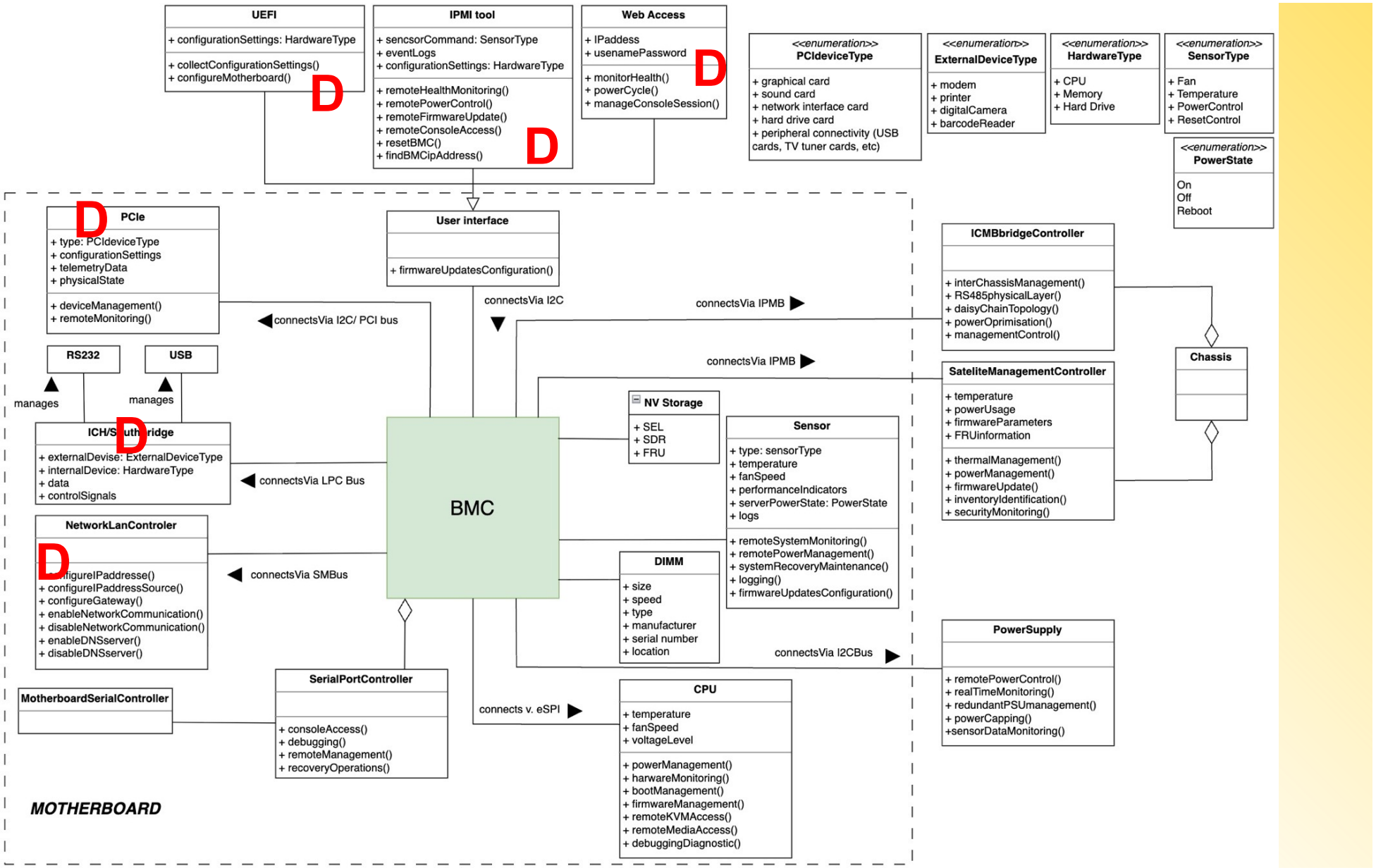

UEFI
+ configurationSettings: HardwareType
+ collectConfigurationSettings()
+ configureMotherboard()
IPMI tool
+ sencsorCommand: SensorType
+ eventLogs
+ configurationSettings: HardwareType
+ remoteHealthMonitoring()
+ remotePowerControl()
+ remoteFirmwareUpdate()
+ remoteConsoleAccess()
+ resetBMC()
+ findBMCipAddress()
Web Access
+ IPaddess
+ usenamePassword
+ monitorHealth()
+ powerCycle()
+ manageConsoleSession()
<<enumeration>>
PCIdeviceType
+ graphical card
+ sound card
+ network interface card
+ hard drive card
+ peripheral connectivity (USB cards, TV tuner cards, etc)
<<enumeration>>
ExternalDeviceType
+ modem
+ printer
+ digitalCamera
+ barcodeReader
<<enumeration>>
HardwareType
+ CPU
+ Memory
+ Hard Drive
<<enumeration>>
SensorType
+ Fan
+ Temperature
+ PowerControl
+ ResetControl
<<enumeration>>
PowerState
On
Off
Reboot
PCIe
+ type: PCIdeviceType
+ configurationSettings
+ telemetryData
+ physicalState
+ deviceManagement()
+ remoteMonitoring()
User interface
+ firmwareUpdatesConfiguration()
ICMBbridgeController
+ interChassisManagement()
+ RS485physicalLayer()
+ daisyChainTopology()
+ powerOprimisation()
+ managementControl()
Chassis
connectsVia I2C/ PCI bus
connectsVia I2C
connectsVia IPMB
connectsVia IPMB
RS232
USB
manages
manages
SateliteManagementController
+ temperature
+ powerUsage
+ firmwareParameters
+ FRUinformation
+ thermalManagement()
+ powerManagement()
+ firmwareUpdate()
+ inventoryIdentification()
+ securityMonitoring()
NV Storage
+ SEL
+ SDR
+ FRU
ICH/Southbridge
+ externalDevise: ExternalDeviceType
+ internalDevice: HardwareType
+ data
+ controlSignals
connectsVia LPC Bus
BMC
Sensor
+ type: sensorType
+ temperature
+ fanSpeed
+ performanceIndicators
+ serverPowerState: PowerState
+ logs
+ remoteSystemMonitoring()
+ remotePowerManagement()
+ systemRecoveryMaintenance()
+ logging()
+ firmwareUpdatesConfiguration()
NetworkLanControler
+ configureIPaddresse()
+ configureIPaddressSource()
+ configureGateway()
+ enableNetworkCommunication()
+ disableNetworkCommunication()
+ enableDNSserver()
+ disableDNSserver()
connectsVia SMBus
DIMM
+ size
+ speed
+ type
+ manufacturer
+ serial number
+ location
connectsVia I2CBus
PowerSupply
+ remotePowerControl()
+ realTimeMonitoring()
+ redundantPSUmanagement()
+ powerCapping()
+sensorDataMonitoring()
SerialPortController
+ consoleAccess()
+ debugging()
+ remoteManagement()
+ recoveryOperations()
MotherboardSerialController
connects v. eSPI
CPU
+ temperature
+ fanSpeed
+ voltageLevel
+ powerManagement()
+ harwareMonitoring()
+ bootManagement()
+ firmwareManagement()
+ remoteKVMAccess()
+ remoteMediaAccess()
+ debuggingDiagnostic()
MOTHERBOARD


UEFI
+ configurationSettings: HardwareType
+ collectConfigurationSettings()
+ configureMotherboard()
IPMI tool
+ sencsorCommand: SensorType
+ eventLogs
+ configurationSettings: HardwareType
+ remoteHealthMonitoring()
+ remotePowerControl()
+ remoteFirmwareUpdate()
+ remoteConsoleAccess()
+ resetBMC()
+ findBMCipAddress()
Web Access
+ IPaddess
+ usenamePassword
+ monitorHealth()
+ powerCycle()
+ manageConsoleSession()
<<enumeration>>
PCIdeviceType
+ graphical card
+ sound card
+ network interface card
+ hard drive card
+ peripheral connectivity (USB cards, TV tuner cards, etc)
<<enumeration>>
ExternalDeviceType
+ modem
+ printer
+ digitalCamera
+ barcodeReader
<<enumeration>>
HardwareType
+ CPU
+ Memory
+ Hard Drive
<<enumeration>>
SensorType
+ Fan
+ Temperature
+ PowerControl
+ ResetControl
<<enumeration>>
PowerState
On
Off
Reboot
PCIe
+ type: PCIdeviceType
+ configurationSettings
+ telemetryData
+ physicalState
+ deviceManagement()
+ remoteMonitoring()
User interface
+ firmwareUpdatesConfiguration()
ICMBbridgeController
+ interChassisManagement()
+ RS485physicalLayer()
+ daisyChainTopology()
+ powerOprimisation()
+ managementControl()
Chassis
connectsVia I2C/ PCI bus
connectsVia I2C
connectsVia IPMB
connectsVia IPMB
RS232
USB
manages
manages
SateliteManagementController
+ temperature
+ powerUsage
+ firmwareParameters
+ FRUinformation
+ thermalManagement()
+ powerManagement()
+ firmwareUpdate()
+ inventoryIdentification()
+ securityMonitoring()
NV Storage
+ SEL
+ SDR
+ FRU
ICH/Southbridge
+ externalDevise: ExternalDeviceType
+ internalDevice: HardwareType
+ data
+ controlSignals
connectsVia LPC Bus
BMC
Sensor
+ type: sensorType
+ temperature
+ fanSpeed
+ performanceIndicators
+ serverPowerState: PowerState
+ logs
+ remoteSystemMonitoring()
+ remotePowerManagement()
+ systemRecoveryMaintenance()
+ logging()
+ firmwareUpdatesConfiguration()
NetworkLanControler
+ configureIPaddresse()
+ configureIPaddressSource()
+ configureGateway()
+ enableNetworkCommunication()
+ disableNetworkCommunication()
+ enableDNSserver()
+ disableDNSserver()
connectsVia SMBus
DIMM
+ size
+ speed
+ type
+ manufacturer
+ serial number
+ location
connectsVia I2CBus
PowerSupply
+ remotePowerControl()
+ realTimeMonitoring()
+ redundantPSUmanagement()
+ powerCapping()
+sensorDataMonitoring()
MotherboardSerialController
SerialPortController
+ consoleAccess()
+ debugging()
+ remoteManagement()
+ recoveryOperations()
connects v. eSPI
CPU
+ temperature
+ fanSpeed
+ voltageLevel
+ powerManagement()
+ harwareMonitoring()
+ bootManagement()
+ firmwareManagement()
+ remoteKVMAccess()
+ remoteMediaAccess()
+ debuggingDiagnostic()
MOTHERBOARD


UEFI
+ configurationSettings: HardwareType
+ collectConfigurationSettings()
+ configureMotherboard()
IPMI tool
+ sencsorCommand: SensorType
+ eventLogs
+ configurationSettings: HardwareType
+ remoteHealthMonitoring()
+ remotePowerControl()
+ remoteFirmwareUpdate()
+ remoteConsoleAccess()
+ resetBMC()
+ findBMCipAddress()
Web Access
+ IPaddess
+ usenamePassword
+ monitorHealth()
+ powerCycle()
+ manageConsoleSession()
<<enumeration>>
PCIdeviceType
+ graphical card
+ sound card
+ network interface card
+ hard drive card
+ peripheral connectivity (USB cards, TV tuner cards, etc)
<<enumeration>>
ExternalDeviceType
+ modem
+ printer
+ digitalCamera
+ barcodeReader
<<enumeration>>
HardwareType
+ CPU
+ Memory
+ Hard Drive
<<enumeration>>
SensorType
+ Fan
+ Temperature
+ PowerControl
+ ResetControl
<<enumeration>>
PowerState
On
Off
Reboot
PCIe
+ type: PCIdeviceType
+ configurationSettings
+ telemetryData
+ physicalState
+ deviceManagement()
+ remoteMonitoring()
User interface
+ firmwareUpdatesConfiguration()
ICMBbridgeController
+ interChassisManagement()
+ RS485physicalLayer()
+ daisyChainTopology()
+ powerOprimisation()
+ managementControl()
Chassis
SateliteManagementController
+ temperature
+ powerUsage
+ firmwareParameters
+ FRUinformation
+ thermalManagement()
+ powerManagement()
+ firmwareUpdate()
+ inventoryIdentification()
+ securityMonitoring()
connectsVia I2C/ PCI bus
connectsVia I2C
connectsVia IPMB
connectsVia IPMB
RS232
USB
manages
manages
ICH/Southbridge
+ externalDevise: ExternalDeviceType
+ internalDevice: HardwareType
+ data
+ controlSignals
connectsVia LPC Bus
NV Storage
+ SEL
+ SD
+ FRU
S
Sensor
+ type: sensorType
+ temperature
+ fanSpeed
+ performanceIndicators
+ serverPowerState: PowerState
+ logs
+ remoteSystemMonitoring()
+ remotePowerManagement()
+ systemRecoveryMaintenance()
+ logging()
+ firmwareUpdatesConfiguration()
BMC
S
NetworkLanControler
+ configureIPaddresse()
+ configureIPaddressSource()
+ configureGateway()
+ enableNetworkCommunication()
+ disableNetworkCommunication()
+ enableDNSserver()
+ disableDNSserver()
connectsVia SMBus
DIMM
+ size
+ speed
+ type
+ manufacturer
+ serial number
+ location
PowerSupply
+ remotePowerControl()
+ realTimeMonitoring()
+ redundantPSUmanagement()
+ powerCapping()
+sensorDataMonitoring()
connectsVia I2CBus
SerialPortController
+ consoleAccess()
+ debugging()
+ remoteManagement()
+ recoveryOperations()
MotherboardSerialController
connects v. eSPI
CPU
+ temperature
+ fanSpeed
+ voltageLevel
+ powerManagement()
+ harwareMonitoring()
+ bootManagement()
+ firmwareManagement()
+ remoteKVMAccess()
+ remoteMediaAccess()
+ debuggingDiagnostic()
MOTHERBOARD


UEFI
+ configurationSettings: HardwareType
+ collectConfigurationSettings()
+ configureMotherboard()
IPMI tool
+ sencsorCommand: SensorType
+ eventLogs
+ configurationSettings: HardwareType
+ remoteHealthMonitoring()
+ remotePowerControl()
+ remoteFirmwareUpdate()
+ remoteConsoleAccess()
+ resetBMC()
+ findBMCipAddress()
Web Access
+ IPaddess
+ usenamePassword
+ monitorHealth()
+ powerCycle()
+ manageConsoleSession()
<<enumeration>>
PCIdeviceType
+ graphical card
+ sound card
+ network interface card
+ hard drive card
+ peripheral connectivity (USB cards, TV tuner cards, etc)
<<enumeration>>
ExternalDeviceType
+ modem
+ printer
+ digitalCamera
+ barcodeReader
<<enumeration>>
HardwareType
+ CPU
+ Memory
+ Hard Drive
<<enumeration>>
SensorType
+ Fan
+ Temperature
+ PowerControl
+ ResetControl
<<enumeration>>
PowerState
On
Off
Reboot
PCIe
+ type: PCIdeviceType
+ configurationSettings
+ telemetryData
+ physicalState
+ deviceManagement()
+ remoteMonitoring()
User interface
+ firmwareUpdatesConfiguration()
ICMBbridgeController
+ interChassisManagement()
+ RS485physicalLayer()
+ daisyChainTopology()
+ powerOprimisation()
+ managementControl()
Chassis
SateliteManagementController
+ temperature
+ powerUsage
+ firmwareParameters
+ FRUinformation
+ thermalManagement()
+ powerManagement()
+ firmwareUpdate()
+ inventoryIdentification()
+ securityMonitoring()
connectsVia I2C/ PCI bus
connectsVia I2C
connectsVia IPMB
connectsVia IPMB
RS232
USB
manages
manages
ICH/Southbridge
+ externalDevise: ExternalDeviceType
+ internalDevice: HardwareType
+ data
+ controlSignals
connectsVia LPC Bus
NV Storage
+ SEL
+ SDR
+ FRU
R
Sensor
+ type: sensorType
+ temperature
+ fanSpeed
+ performanceIndicators
+ serverPowerState: PowerState
+ logs
+ remoteSystemMonitoring()
+ remotePowerManagement()
+ systemRecoveryMaintenance()
+ logging()
+ firmwareUpdatesConfiguration()
BMC
R
NetworkLanControler
+ configureIPaddresse()
+ configureIPaddressSource()
+ configureGateway()
+ enableNetworkCommunication()
+ disableNetworkCommunication()
+ enableDNSserver()
+ disableDNSserver()
connectsVia SMBus
DIMM
+ size
+ speed
+ type
+ manufacturer
+ serial number
+ location
PowerSupply
+ remotePowerControl()
+ realTimeMonitoring()
+ redundantPSUmanagement()
+ powerCapping()
+sensorDataMonitoring()
connectsVia I2CBus
SerialPortController
+ consoleAccess()
+ debugging()
+ remoteManagement()
+ recoveryOperations()
MotherboardSerialController
connects v. eSPI
CPU
+ temperature
+ fanSpeed
+ voltageLevel
+ powerManagement()
+ harwareMonitoring()
+ bootManagement()
+ firmwareManagement()
+ remoteKVMAccess()
+ remoteMediaAccess()
+ debuggingDiagnostic()
MOTHERBOARD


UEFI
+ configurationSettings: HardwareType
+ collectConfigurationSettings()
+ configureMotherboard()
IPMI tool
+ sencsorCommand: SensorType
+ eventLogs
+ configurationSettings: HardwareType
+ remoteHealthMonitoring()
+ remotePowerControl()
+ remoteFirmwareUpdate()
+ remoteConsoleAccess()
+ resetBMC()
+ findBMCipAddress()
Web Access
+ IPaddess
+ usenamePassword
+ monitorHealth()
+ powerCycle()
+ manageConsoleSession()
<<enumeration>>
PCIdeviceType
+ graphical card
+ sound card
+ network interface card
+ hard drive card
+ peripheral connectivity (USB cards, TV tuner cards, etc)
<<enumeration>>
ExternalDeviceType
+ modem
+ printer
+ digitalCamera
+ barcodeReader
<<enumeration>>
HardwareType
+ CPU
+ Memory
+ Hard Drive
<<enumeration>>
SensorType
+ Fan
+ Temperature
+ PowerControl
+ ResetControl
<<enumeration>>
PowerState
On
Off
Reboot
PCIe
+ type: PCIdeviceType
+ configurationSettings
+ telemetryData
+ physicalState
+ deviceManagement()
+ remoteMonitoring()
M
User interface
+ firmwareUpdatesConfiguration()
connectsVia I2C/ PCI bus
connectsVia I2C
connectsVia IPMB
connectsVia IPMB
ICMBbridgeController
+ interChassisManagement()
+ RS485physicalLayer()
+ daisyChainTopology()
+ powerOprimisation()
+ managementControl()
Chassis
SateliteManagementController
+ FRUinformation
+ thermalManagement()
+ powerManagement()
+ firmwareUpdate()
+ inventoryIdentification()
+ securityMonitoring()
M
RS232
USB
manages
manages
ICH/Southbridge
+ externalDevise: ExternalDeviceType
+ internalDevice: HardwareType
+ data
+ controlSignals
connectsVia LPC Bus
NV Storage
+ SEL
+ SDR
+ FRU
Sensor
+ type: sensorType
+ temperature
+ fanSpeed
+ performanceIndicators
+ serverPowerState: PowerState
+ logs
+ remoteSystemMonitoring()
+ remotePowerManagement()
+ systemRecoveryMaintenance()
+ logging()
+ firmwareUpdatesConfiguration()
BMC
M
NetworkLanControler
+ configureIPaddresse()
+ configureIPaddressSource()
+ configureGateway()
+ enableNetworkCommunication()
+ disableNetworkCommunication()
+ enableDNSserver()
+ disableDNSserver()
M
connectsVia SMBus
DIMM
+ size
+ speed
+ type
+ manufacturer
+ serial number
+ location
connectsVia I2CBus
PowerSupply
+ realTimeMonitoring()
+ redundantPSUmanagement()
+ powerCapping()
+sensorDataMonitoring()
M
SerialPortController
+ consoleAccess()
+ debugging()
+ remoteManagement()
+ recoveryOperations()
M
MotherboardSerialController
connects v. eSPI
CPU
+ temperature
+ fanSpeed
+ voltageLevel
+ powerManagement()
+ harwareMonitoring()
+ bootManagement()
+ firmwareManagement()
+ remoteKVMAccess()
+ remoteMediaAccess()
+ debuggingDiagnostic()
M
MOTHERBOARD


UEFI
+ configurationSettings: HardwareType
+ collectConfigurationSettings()
+ configureMotherboard()
IPMI tool
+ sencsorCommand: SensorType
+ eventLogs
+ configurationSettings: HardwareType
+ remoteHealthMonitoring()
+ remotePowerControl()
+ remoteFirmwareUpdate()
+ remoteConsoleAccess()
+ resetBMC()
+ findBMCipAddress()
Web Access
+ IPaddess
+ usenamePassword
+ monitorHealth()
+ powerCycle()
+ manageConsoleSession()
<<enumeration>>
PCIdeviceType
+ graphical card
+ sound card
+ network interface card
+ hard drive card
+ peripheral connectivity (USB cards, TV tuner cards, etc)
<<enumeration>>
ExternalDeviceType
+ modem
+ printer
+ digitalCamera
+ barcodeReader
<<enumeration>>
HardwareType
+ CPU
+ Memory
+ Hard Drive
<<enumeration>>
SensorType
+ Fan
+ Temperature
+ PowerControl
+ ResetControl
<<enumeration>>
PowerState
On
Off
Reboot
PCIe
+ type: PCIdeviceType
+ configurationSettings
+ telemetryData
+ physicalState
+ deviceManagement()
+ remoteMonitoring()
User interface
+ firmwareUpdatesConfiguration()
ICMBbridgeController
+ interChassisManagement()
+ RS485physicalLayer()
+ daisyChainTopology()
+ powerOprimisation()
+ managementControl()
Chassis
connectsVia I2C/ PCI bus
connectsVia I2C
connectsVia IPMB
connectsVia IPMB
RS232
USB
manages
manages
SateliteManagementController
+ temperature
+ powerUsage
+ firmwareParameters
+ FRUinformation
+ thermalManagement()
+ powerManagement()
+ firmwareUpdate()
+ inventoryIdentification()
+ securityMonitoring()
NV Storage
+ SEL
+ SDR
+ FRU
ICH/Southbridge
+ externalDevise: ExternalDeviceType
+ internalDevice: HardwareType
+ data
+ controlSignals
connectsVia LPC Bus
BMC
Sensor
+ type: sensorType
+ temperature
+ fanSpeed
+ performanceIndicators
+ serverPowerState: PowerState
+ logs
+ remoteSystemMonitoring()
+ remotePowerManagement()
+ systemRecoveryMaintenance()
+ logging()
+ firmwareUpdatesConfiguration()
NetworkLanControler
+ configureIPaddresse()
+ configureIPaddressSource()
+ configureGateway()
+ enableNetworkCommunication()
+ disableNetworkCommunication()
+ enableDNSserver()
+ disableDNSserver()
connectsVia SMBus
DIMM
+ size
+ speed
+ type
+ manufacturer
+ serial number
+ location
PowerSupply
+ remotePowerControl()
+ realTimeMonitoring()
+ redundantPSUmanagement()
+ powerCapping()
+sensorDataMonitoring()
connectsVia I2CBus
SerialPortController
+ consoleAccess()
+ debugging()
+ remoteManagement()
+ recoveryOperations()
MotherboardSerialController
connects v. eSPI
CPU
+ temperature
+ fanSpeed
+ voltageLevel
+ powerManagement()
+ harwareMonitoring()
+ bootManagement()
+ firmwareManagement()
+ remoteKVMAccess()
+ remoteMediaAccess()
+ debuggingDiagnostic()
MOTHERBOARD

Adversarial Model

- Opportunistic Internet-based attack
- Targeted intranet-based attack
- Targeted host-based attack

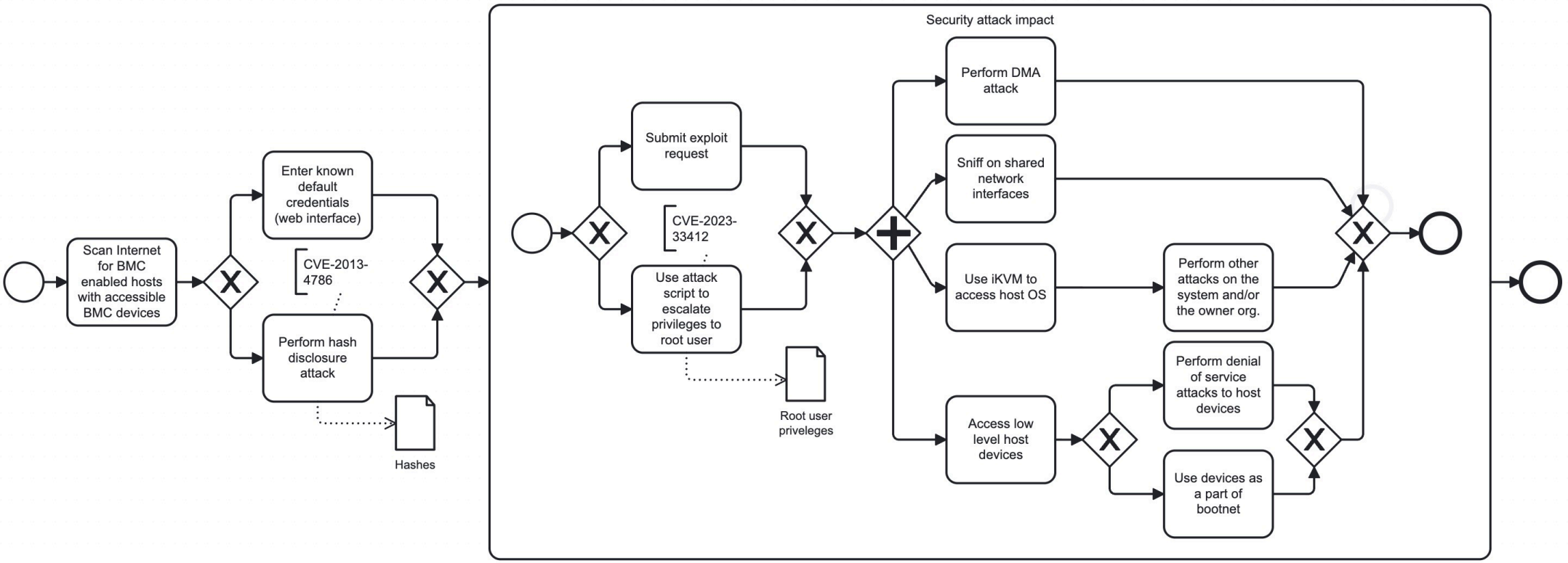
Ahti Pellinen, Baseboard management controller vulnerabilities, misconfigurations, and exploitation. A case study of Supermicro X11-based BMC security, Master's thesis, Jyväskylä: JAMK University of Applied Sciences, December 2023, 75 pp

Adversarial Model

- Opportunistic Internet-based attack
- Targeted intranet-based attack
- Targeted host-based attack

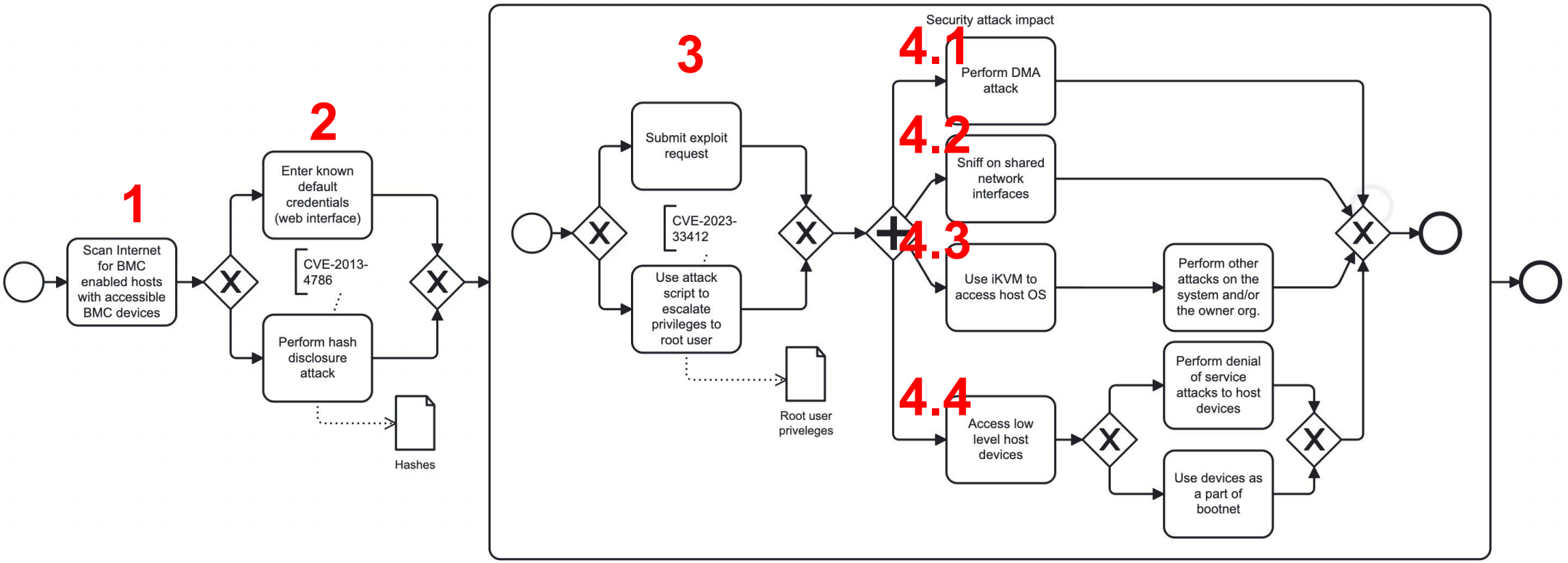
Ahti Pellinen, Baseboard management controller vulnerabilities, misconfigurations, and exploitation. A case study of Supermicro X11-based BMC security, Master's thesis, Jyväskylä: JAMK University of Applied Sciences, December 2023, 75 pp

Opportunistic Internet-based attack

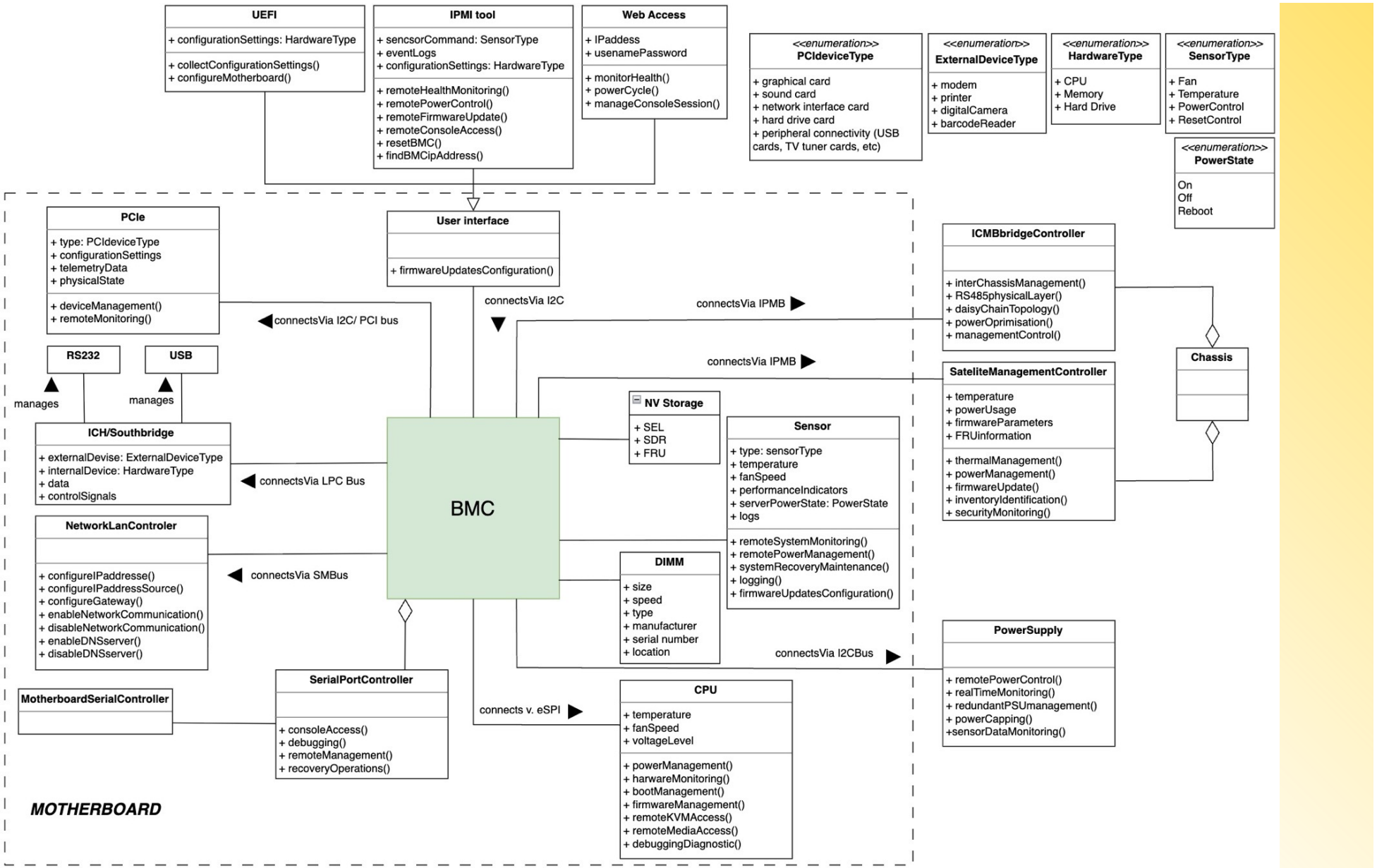


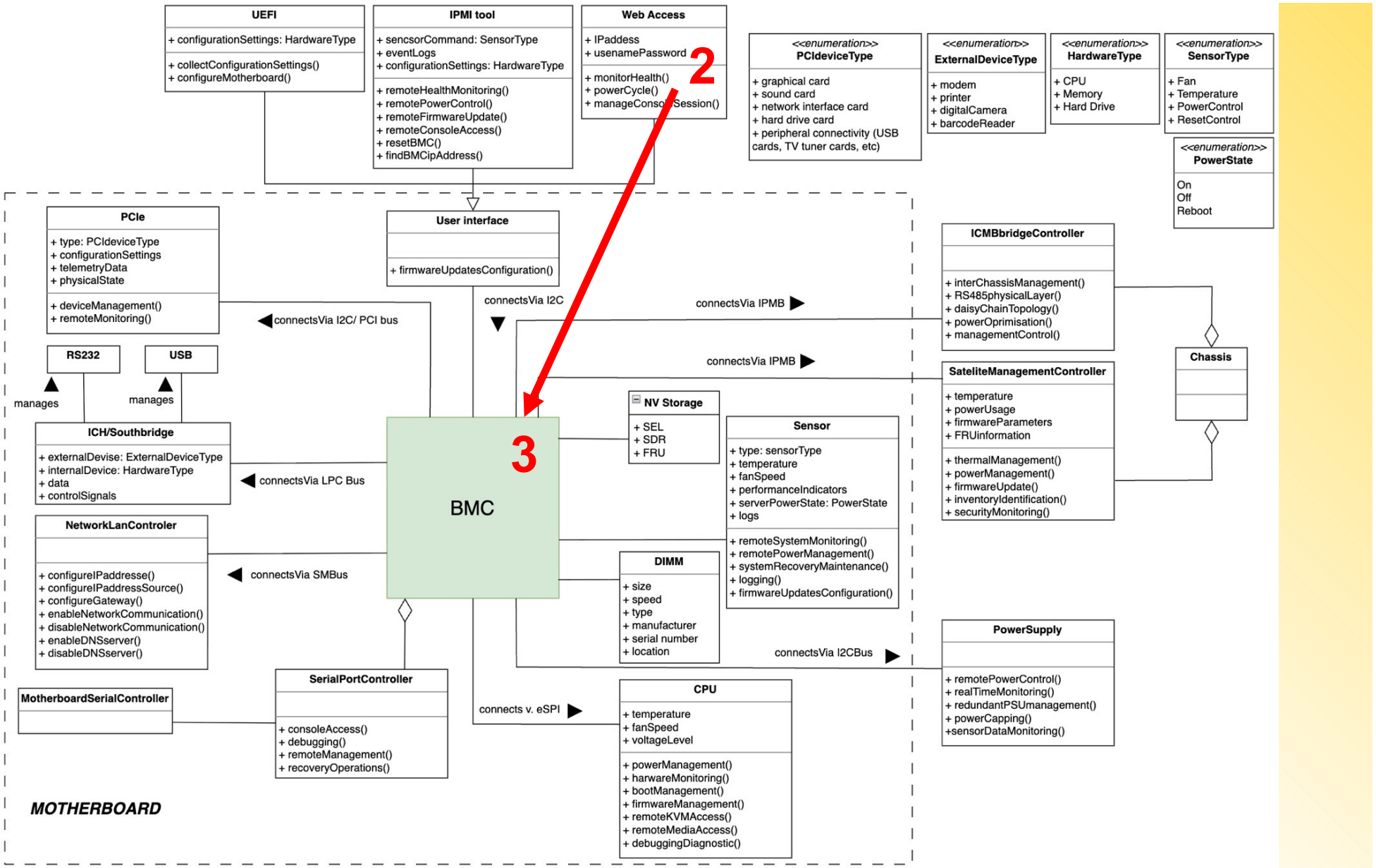
Ahti Pellinen, Baseboard management controller vulnerabilities, misconfigurations, and exploitation. A case study of Supermicro X11-based BMC security, Master's thesis, Jyväskylä: JAMK University of Applied Sciences, December 2023, 75 pp

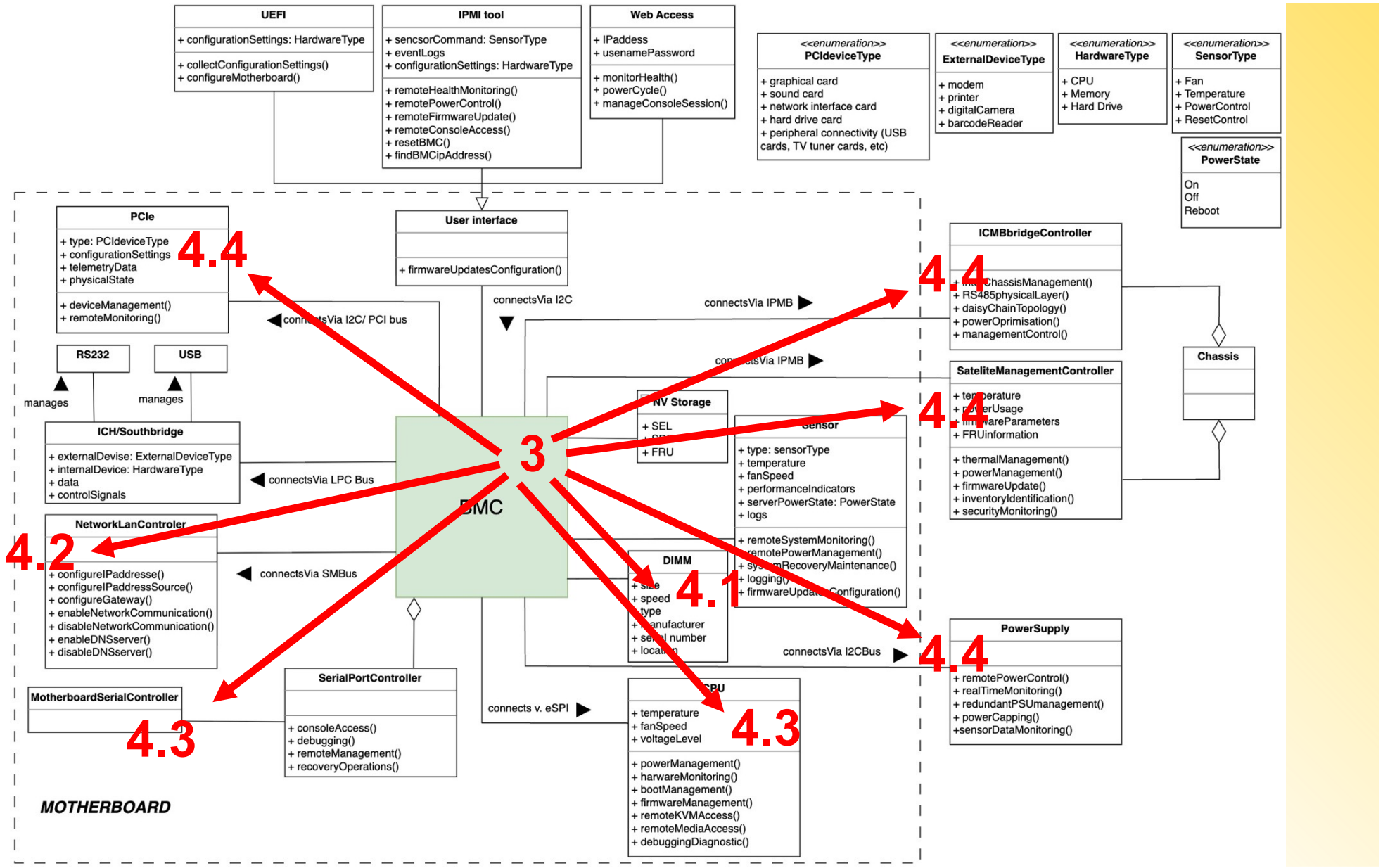
Opportunistic Internet-based attack



Ahti Pellinen, Baseboard management controller vulnerabilities, misconfigurations, and exploitation. A case study of Supermicro X11-based BMC security, Master's thesis, Jyväskylä: JAMK University of Applied Sciences, December 2023, 75 pp


UEFI
+ configurationSettings: HardwareType
+ collectConfigurationSettings()
+ configureMotherboard()
IPMI tool
+ sencsorCommand: SensorType
+ eventLogs
+ configurationSettings: HardwareType
+ remoteHealthMonitoring()
+ remotePowerControl()
+ remoteFirmwareUpdate()
+ remoteConsoleAccess()
+ resetBMC()
+ findBMCipAddress()
Web Access
+ IPaddess
+ usenamePassword
+ monitorHealth()
+ powerCycle()
+ manageConsoleSession()
<<enumeration>>
PCIdeviceType
+ graphical card
+ sound card
+ network interface card
+ hard drive card
+ peripheral connectivity (USB cards, TV tuner cards, etc)
<<enumeration>>
ExternalDeviceType
+ modem
+ printer
+ digitalCamera
+ barcodeReader
<<enumeration>>
HardwareType
+ CPU
+ Memory
+ Hard Drive
<<enumeration>>
SensorType
+ Fan
+ Temperature
+ PowerControl
+ ResetControl
<<enumeration>>
PowerState
On
Off
Reboot
PCIe
+ type: PCIdeviceType
+ configurationSettings
+ telemetryData
+ physicalState
+ deviceManagement()
+ remoteMonitoring()
User interface
+ firmwareUpdatesConfiguration()
ICMBbridgeController
+ interChassisManagement()
+ RS485physicalLayer()
+ daisyChainTopology()
+ powerOprimisation()
+ managementControl()
Chassis
SateliteManagementController
+ temperature
+ powerUsage
+ firmwareParameters
+ FRUinformation
+ thermalManagement()
+ powerManagement()
+ firmwareUpdate()
+ inventoryIdentification()
+ securityMonitoring()
connectsVia I2C/ PCI bus
connectsVia I2C
connectsVia IPMB
connectsVia IPMB
RS232
USB
manages
manages
ICH/Southbridge
+ externalDevise: ExternalDeviceType
+ internalDevice: HardwareType
+ data
+ controlSignals
connectsVia LPC Bus
BMC
NV Storage
+ SEL
+ SDR
+ FRU
Sensor
+ type: sensorType
+ temperature
+ fanSpeed
+ performanceIndicators
+ serverPowerState: PowerState
+ logs
+ remoteSystemMonitoring()
+ remotePowerManagement()
+ systemRecoveryMaintenance()
+ logging()
+ firmwareUpdatesConfiguration()
NetworkLanControler
+ configureIPaddresse()
+ configureIPaddressSource()
+ configureGateway()
+ enableNetworkCommunication()
+ disableNetworkCommunication()
+ enableDNSserver()
+ disableDNSserver()
connectsVia SMBus
DIMM
+ size
+ speed
+ type
+ manufacturer
+ serial number
+ location
PowerSupply
+ remotePowerControl()
+ realTimeMonitoring()
+ redundantPSUmanagement()
+ powerCapping()
+sensorDataMonitoring()
connectsVia I2CBus
SerialPortController
+ consoleAccess()
+ debugging()
+ remoteManagement()
+ recoveryOperations()
MotherboardSerialController
connects v. eSPI
CPU
+ temperature
+ fanSpeed
+ voltageLevel
+ powerManagement()
+ harwareMonitoring()
+ bootManagement()
+ firmwareManagement()
+ remoteKVMAccess()
+ remoteMediaAccess()
+ debuggingDiagnostic()
MOTHERBOARD


UEFI
+ configurationSettings: HardwareType
+ collectConfigurationSettings()
+ configureMotherboard()
IPMI tool
+ sencsorCommand: SensorType
+ eventLogs
+ configurationSettings: HardwareType
+ remoteHealthMonitoring()
+ remotePowerControl()
+ remoteFirmwareUpdate()
+ remoteConsoleAccess()
+ resetBMC()
+ findBMCipAddress()
Web Access
+ IPaddess
+ usenamePassword
+ monitorHealth()
+ powerCycle()
+ manageConsoleSession()
2
<<enumeration>>
PCIdeviceType
+ graphical card
+ sound card
+ network interface card
+ hard drive card
+ peripheral connectivity (USB cards, TV tuner cards, etc)
<<enumeration>>
ExternalDeviceType
+ modem
+ printer
+ digitalCamera
+ barcodeReader
<<enumeration>>
HardwareType
+ CPU
+ Memory
+ Hard Drive
<<enumeration>>
SensorType
+ Fan
+ Temperature
+ PowerControl
+ ResetControl
<<enumeration>>
PowerState
On
Off
Reboot
PCIe
+ type: PCIdeviceType
+ configurationSettings
+ telemetryData
+ physicalState
+ deviceManagement()
+ remoteMonitoring()
User interface
+ firmwareUpdatesConfiguration()
ICMBbridgeController
+ interChassisManagement()
+ RS485physicalLayer()
+ daisyChainTopology()
+ powerOprimisation()
+ managementControl()
Chassis
SateliteManagementController
+ temperature
+ powerUsage
+ firmwareParameters
+ FRUinformation
+ thermalManagement()
+ powerManagement()
+ firmwareUpdate()
+ inventoryIdentification()
+ securityMonitoring()
connectsVia I2C/ PCI bus
connectsVia I2C
connectsVia IPMB
connectsVia IPMB
RS232
USB
manages
manages
ICH/Southbridge
+ externalDevise: ExternalDeviceType
+ internalDevice: HardwareType
+ data
+ controlSignals
connectsVia LPC Bus
3
BMC
NV Storage
+ SEL
+ SDR
+ FRU
Sensor
+ type: sensorType
+ temperature
+ fanSpeed
+ performanceIndicators
+ serverPowerState: PowerState
+ logs
+ remoteSystemMonitoring()
+ remotePowerManagement()
+ systemRecoveryMaintenance()
+ logging()
+ firmwareUpdatesConfiguration()
NetworkLanControler
+ configureIPaddresse()
+ configureIPaddressSource()
+ configureGateway()
+ enableNetworkCommunication()
+ disableNetworkCommunication()
+ enableDNSserver()
+ disableDNSserver()
connectsVia SMBus
DIMM
+ size
+ speed
+ type
+ manufacturer
+ serial number
+ location
connectsVia I2CBus
PowerSupply
+ remotePowerControl()
+ realTimeMonitoring()
+ redundantPSUmanagement()
+ powerCapping()
+sensorDataMonitoring()
MotherboardSerialController
SerialPortController
+ consoleAccess()
+ debugging()
+ remoteManagement()
+ recoveryOperations()
connects v. eSPI
CPU
+ temperature
+ fanSpeed
+ voltageLevel
+ powerManagement()
+ harwareMonitoring()
+ bootManagement()
+ firmwareManagement()
+ remoteKVMAccess()
+ remoteMediaAccess()
+ debuggingDiagnostic()
MOTHERBOARD


UEFI
+ configurationSettings: HardwareType
+ collectConfigurationSettings()
+ configureMotherboard()
IPMI tool
+ sencsorCommand: SensorType
+ eventLogs
+ configurationSettings: HardwareType
+ remoteHealthMonitoring()
+ remotePowerControl()
+ remoteFirmwareUpdate()
+ remoteConsoleAccess()
+ resetBMC()
+ findBMCipAddress()
Web Access
+ IPaddess
+ usenamePassword
+ monitorHealth()
+ powerCycle()
+ manageConsoleSession()
<<enumeration>>
PCIdeviceType
+ graphical card
+ sound card
+ network interface card
+ hard drive card
+ peripheral connectivity (USB cards, TV tuner cards, etc)
<<enumeration>>
ExternalDeviceType
+ modem
+ printer
+ digitalCamera
+ barcodeReader
<<enumeration>>
HardwareType
+ CPU
+ Memory
+ Hard Drive
<<enumeration>>
SensorType
+ Fan
+ Temperature
+ PowerControl
+ ResetControl
<<enumeration>>
PowerState
On
Off
Reboot
PCIe
+ type: PCIdeviceType
+ configurationSettings
+ telemetryData
+ physicalState
+ deviceManagement()
+ remoteMonitoring()
4.4
User interface
+ firmwareUpdatesConfiguration()
connectsVia I2C
connectsVia IPMB
connectsVia I2C/ PCI bus
connectsVia IPMB
ICMBbridgeController
+ RS485physicalLayer()
+ daisyChainTopology()
+ powerOprimisation()
+ managementControl()
Chassis
SateliteManagementController
+ FRUinformation
+ thermalManagement()
+ powerManagement()
+ firmwareUpdate()
+ inventoryIdentification()
+ securityMonitoring()
RS232
USB
manages
manages
ICH/Southbridge
+ externalDevise: ExternalDeviceType
+ internalDevice: HardwareType
+ data
+ controlSignals
connectsVia LPC Bus
NV Storage
+ SEL
+ FRU
Sensor
+ type: sensorType
+ temperature
+ fanSpeed
+ performanceIndicators
+ serverPowerState: PowerState
+ logs
+ remoteSystemMonitoring()
+ remotePowerManagement()
+ logging()
+ firmwareUpdateConfiguration()
3
BMC
NetworkLanControler
+ configureIPaddresse()
+ configureIPaddressSource()
+ configureGateway()
+ enableNetworkCommunication()
+ disableNetworkCommunication()
+ enableDNSserver()
+ disableDNSserver()
4.2
connectsVia SMBus
DIMM
+ speed
+ type
+ manufacturer
4.1
connectsVia I2CBus
PowerSupply
+ remotePowerControl()
+ realTimeMonitoring()
+ redundantPSUmanagement()
+ powerCapping()
+sensorDataMonitoring()
4.4
MotherboardSerialController
4.3
SerialPortController
+ consoleAccess()
+ debugging()
+ remoteManagement()
+ recoveryOperations()
connects v. eSPI
CPU
+ temperature
+ fanSpeed
+ voltageLevel
+ powerManagement()
+ harwareMonitoring()
+ bootManagement()
+ firmwareManagement()
+ remoteKVMAccess()
+ remoteMediaAccess()
+ debuggingDiagnostic()
4.3
MOTHERBOARD

Adversarial Model

Critical assets

Attack Surface Enumeration

Adversarial model

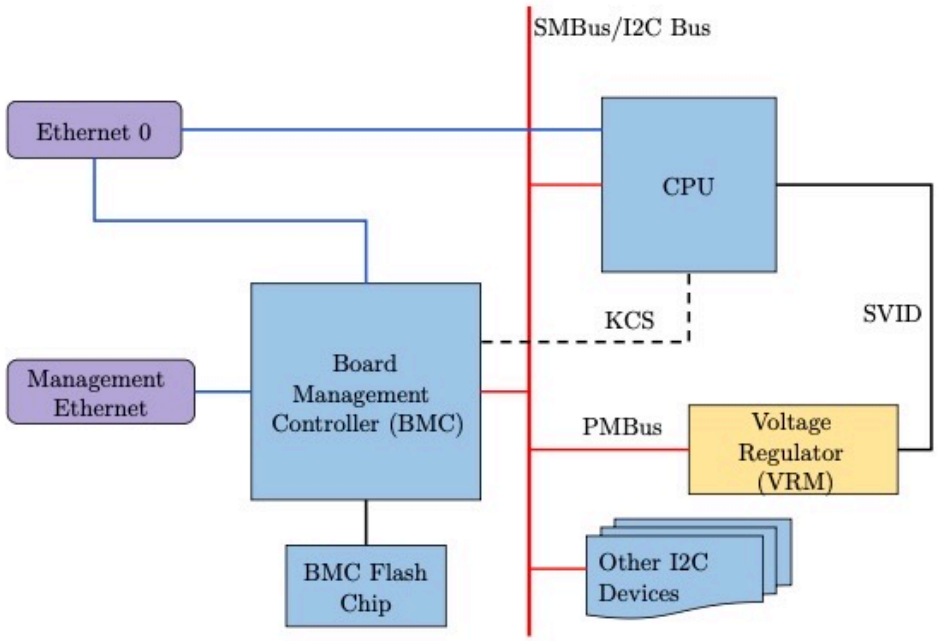
Security Objectives

- Opportunistic Internet-based attack
- Targeted intranet-based attack
- Targeted host-based attack

Ahti Pellinen, Baseboard management controller vulnerabilities, misconfigurations, and exploitation. A case study of Supermicro X11-based BMC security, Master's thesis, Jyväskylä: JAMK University of Applied Sciences, December 2023, 75 pp

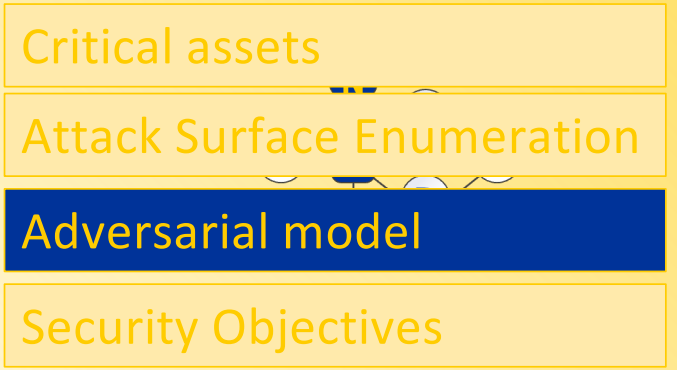
PMFault: Faulting and Bricking Server CPUs through Management Interfaces

- Critical assets
- Attack Surface Enumeration
- **Adversarial model**
- Security Objectives



Chen, Z., & Oswald, D. (2023). PMFault: Faulting and Bricking Server CPUs through Management Interfaces: Or: A Modern Example of Halt and Catch Fire. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2023(2), 1-23.

Adversarial Models



Code problem

Configuration errors

- The latest version is not used
- Encryption configuration
- Authentication configuration
- Communication configuration

Security problems in the BMC architecture

- Potential DMA attack
- The interface has security defects
- Fragile update mechanism

Network Attacks

Software modifications

Attacking Firmware from the Operating System

Hardware Upgrades

Establishing Persistence

Option ROM Attack

Direct Memory Access (DMA)

Processor-Level Vulnerability Exploitation

Device Disabling

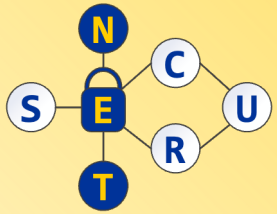
doi: 10.1109/ICET61945.2024.10673073

doi: 10.1109/iThings-GreenCom-CPSCom-SmartData-Cybermatics62450.2024.00026

Security Objectives

- BMC configuration
- Network configuration
- Additional measures

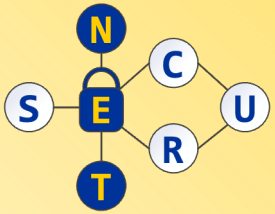
BMC Configuration



- Change the default password during installation
- Create user policies and roles on BMC
- Use the IP Access Policy to enable BMC access from management servers
- Customise notifications and alerts for high-severity event log and maintenance event log entries
- Configure BIOS security features by OOB management
- Configure the BMC management account security feature
- Customise service ports information on the BMC to your data centre specifications
- Configure the BMC lockdown feature

https://www.supermicro.com/products/nfo/files/IPMI/Best_Practices_BMC_Security.pdf

Network and Additional Measures



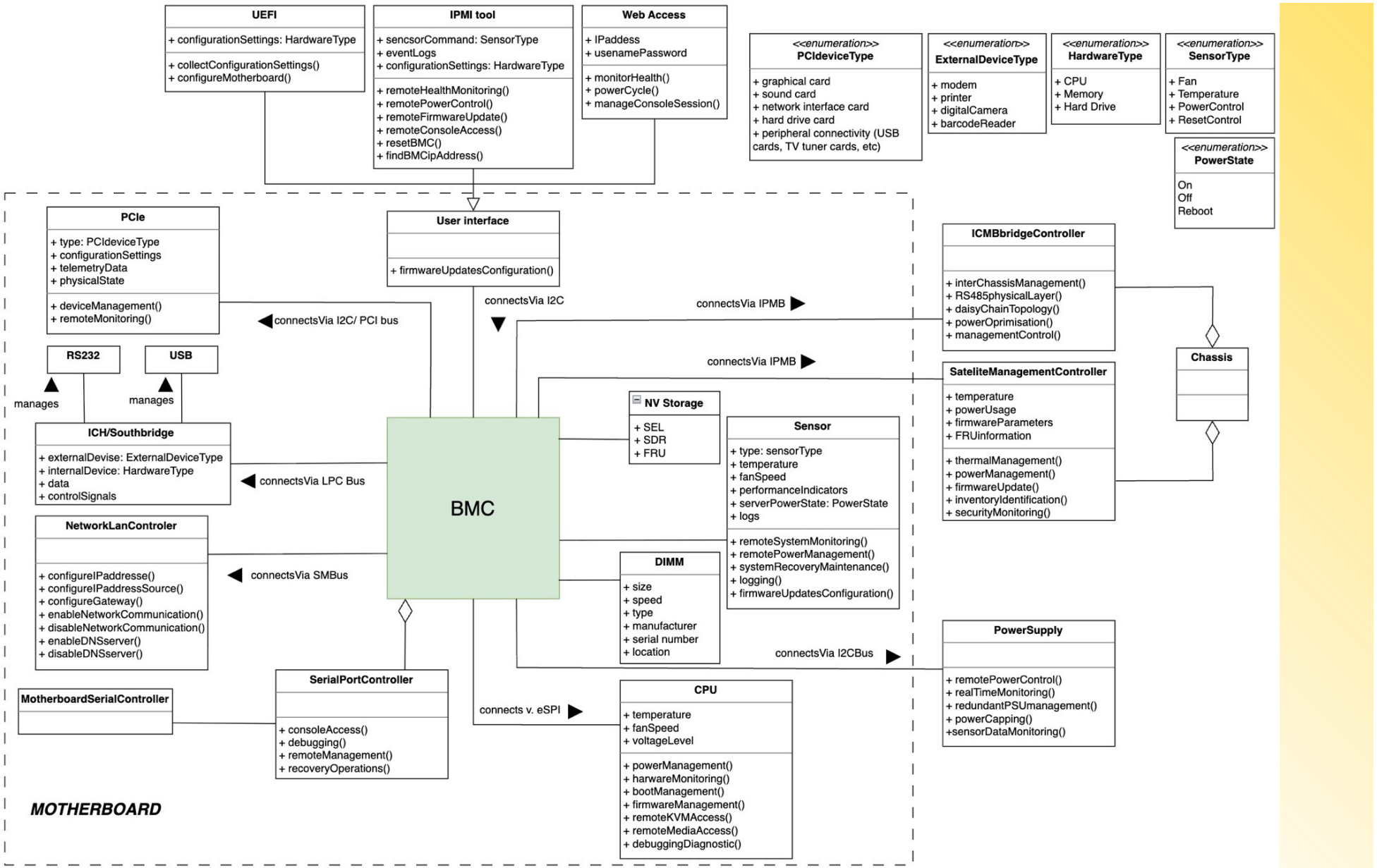
Network configuration

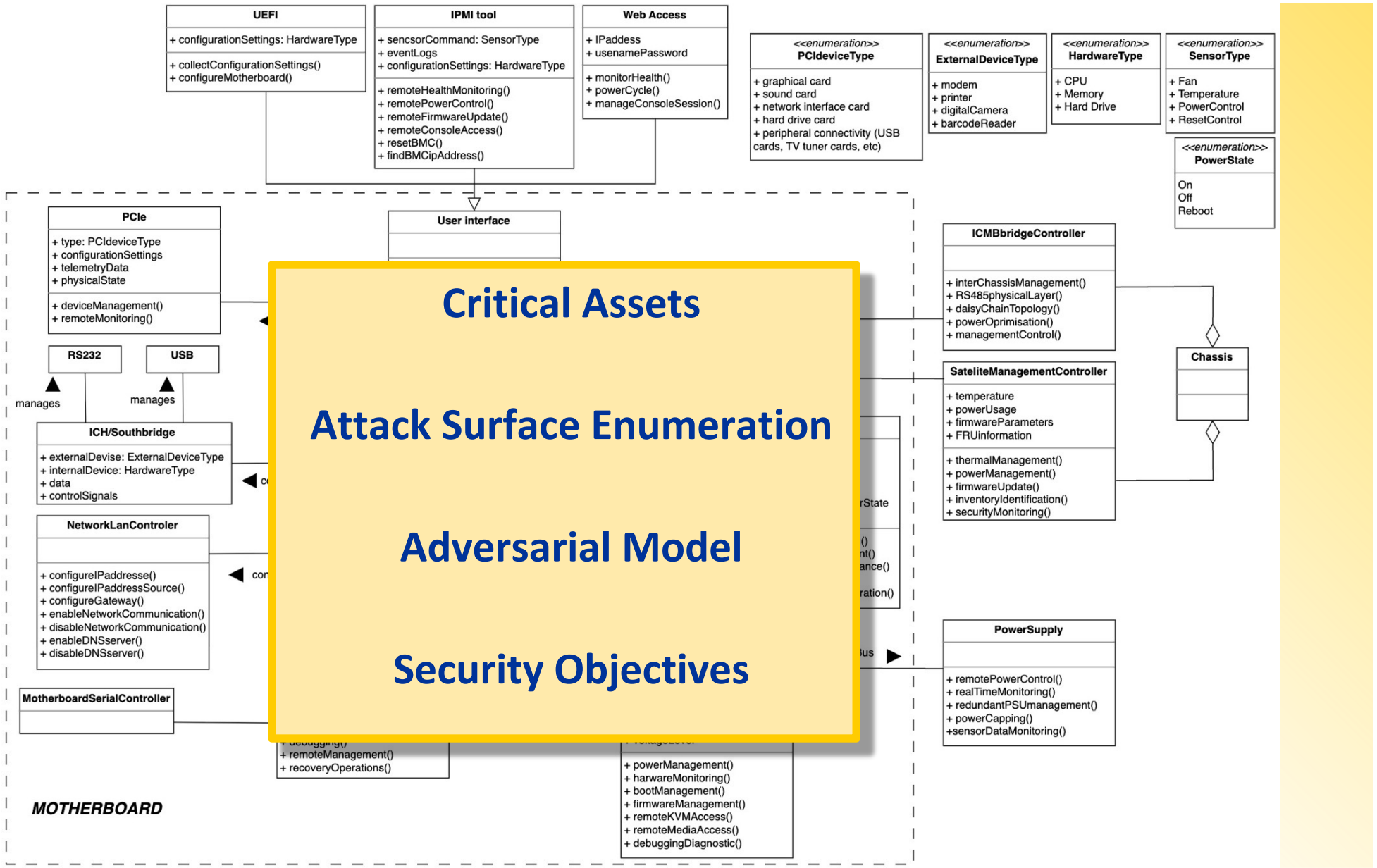
- Restrict inbound traffic over the internet directly to BMCs
- Reserve a special IP address range (private subnets) for BMC management interfaces and management servers
- Configure the firewall to restrict outbound traffic from BMC, including alerts, within the reserved IP range

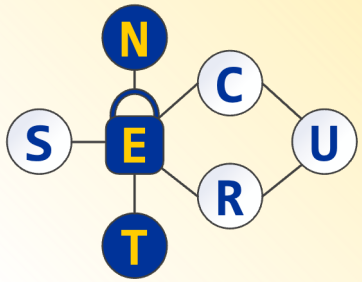
Additional measures

- Monitor for unusual traffic between BMC and other machines in the network
- Pay attention to firmware release notes
  - Especially related to security fixes
  - Plan upgrades of the firmware during maintenance cycles

https://www.supermicro.com/products/nfo/files/IPMI/Best_Practices_BMC_Security.pdf


UEFI
+ configurationSettings: HardwareType
+ collectConfigurationSettings()
+ configureMotherboard()
IPMI tool
+ sencsorCommand: SensorType
+ eventLogs
+ configurationSettings: HardwareType
+ remoteHealthMonitoring()
+ remotePowerControl()
+ remoteFirmwareUpdate()
+ remoteConsoleAccess()
+ resetBMC()
+ findBMCipAddress()
Web Access
+ IPaddess
+ usenamePassword
+ monitorHealth()
+ powerCycle()
+ manageConsoleSession()
<<enumeration>>
PCIdeviceType
+ graphical card
+ sound card
+ network interface card
+ hard drive card
+ peripheral connectivity (USB cards, TV tuner cards, etc)
<<enumeration>>
ExternalDeviceType
+ modem
+ printer
+ digitalCamera
+ barcodeReader
<<enumeration>>
HardwareType
+ CPU
+ Memory
+ Hard Drive
<<enumeration>>
SensorType
+ Fan
+ Temperature
+ PowerControl
+ ResetControl
<<enumeration>>
PowerState
On
Off
Reboot
PCIe
+ type: PCIdeviceType
+ configurationSettings
+ telemetryData
+ physicalState
+ deviceManagement()
+ remoteMonitoring()
User interface
+ firmwareUpdatesConfiguration()
ICMBbridgeController
+ interChassisManagement()
+ RS485physicalLayer()
+ daisyChainTopology()
+ powerOprimisation()
+ managementControl()
Chassis
SateliteManagementController
+ temperature
+ powerUsage
+ firmwareParameters
+ FRUinformation
+ thermalManagement()
+ powerManagement()
+ firmwareUpdate()
+ inventoryIdentification()
+ securityMonitoring()
connectsVia I2C/ PCI bus
connectsVia I2C
connectsVia IPMB
connectsVia IPMB
RS232
USB
manages
manages
ICH/Southbridge
+ externalDevise: ExternalDeviceType
+ internalDevice: HardwareType
+ data
+ controlSignals
connectsVia LPC Bus
BMC
NV Storage
+ SEL
+ SDR
+ FRU
Sensor
+ type: sensorType
+ temperature
+ fanSpeed
+ performanceIndicators
+ serverPowerState: PowerState
+ logs
+ remoteSystemMonitoring()
+ remotePowerManagement()
+ systemRecoveryMaintenance()
+ logging()
+ firmwareUpdatesConfiguration()
NetworkLanControler
+ configureIPaddresse()
+ configureIPaddressSource()
+ configureGateway()
+ enableNetworkCommunication()
+ disableNetworkCommunication()
+ enableDNSserver()
+ disableDNSserver()
connectsVia SMBus
DIMM
+ size
+ speed
+ type
+ manufacturer
+ serial number
+ location
PowerSupply
+ remotePowerControl()
+ realTimeMonitoring()
+ redundantPSUmanagement()
+ powerCapping()
+sensorDataMonitoring()
connectsVia I2CBus
SerialPortController
+ consoleAccess()
+ debugging()
+ remoteManagement()
+ recoveryOperations()
MotherboardSerialController
connects v. eSPI
CPU
+ temperature
+ fanSpeed
+ voltageLevel
+ powerManagement()
+ harwareMonitoring()
+ bootManagement()
+ firmwareManagement()
+ remoteKVMAccess()
+ remoteMediaAccess()
+ debuggingDiagnostic()
MOTHERBOARD


UEFI
+ configurationSettings: HardwareType
+ collectConfigurationSettings()
+ configureMotherboard()
IPMI tool
+ sencsorCommand: SensorType
+ eventLogs
+ configurationSettings: HardwareType
+ remoteHealthMonitoring()
+ remotePowerControl()
+ remoteFirmwareUpdate()
+ remoteConsoleAccess()
+ resetBMC()
+ findBMCipAddress()
Web Access
+ IPaddess
+ usenamePassword
+ monitorHealth()
+ powerCycle()
+ manageConsoleSession()
<<enumeration>>
PCIdeviceType
+ graphical card
+ sound card
+ network interface card
+ hard drive card
+ peripheral connectivity (USB cards, TV tuner cards, etc)
<<enumeration>>
ExternalDeviceType
+ modem
+ printer
+ digitalCamera
+ barcodeReader
<<enumeration>>
HardwareType
+ CPU
+ Memory
+ Hard Drive
<<enumeration>>
SensorType
+ Fan
+ Temperature
+ PowerControl
+ ResetControl
<<enumeration>>
PowerState
On
Off
Reboot
PCIe
+ type: PCIdeviceType
+ configurationSettings
+ telemetryData
+ physicalState
+ deviceManagement()
+ remoteMonitoring()
User interface
ICMBbridgeController
+ interChassisManagement()
+ RS485physicalLayer()
+ daisyChainTopology()
+ powerOprimisation()
+ managementControl()
Chassis
SateliteManagementController
+ temperature
+ powerUsage
+ firmwareParameters
+ FRUinformation
+ thermalManagement()
+ powerManagement()
+ firmwareUpdate()
+ inventoryIdentification()
+ securityMonitoring()
RS232
USB
manages
manages
ICH/Southbridge
+ externalDevise: ExternalDeviceType
+ internalDevice: HardwareType
+ data
+ controlSignals
NetworkLanControler
+ configureIPaddresse()
+ configureIPaddressSource()
+ configureGateway()
+ enableNetworkCommunication()
+ disableNetworkCommunication()
+ enableDNSserver()
+ disableDNSserver()
MotherboardSerialController
PowerSupply
+ remotePowerControl()
+ realTimeMonitoring()
+ redundantPSUmanagement()
+ powerCapping()
+sensorDataMonitoring()
+ remoteManagement()
+ recoveryOperations()
+ powerManagement()
+ harwareMonitoring()
+ bootManagement()
+ firmwareManagement()
+ remoteKVMAccess()
+ remoteMediaAccess()
+ debuggingDiagnostic()
MOTHERBOARD
Critical Assets
Attack Surface Enumeration
Adversarial Model
Security Objectives



Enhancing Cross-Sectoral Collaboration in Cybersecurity in Estonia, Czechia, Lithuania, Ukraine, and the Netherlands

Funded by the European Union

Website:

https://securenet.isk.ktu.lt/

Facebook:

https://www.facebook.com/enhancing.collaboration.in.cybersecurity/

LinkedIn:

https://www.linkedin.com/company/109759990/admin/dashboard/

Funded by the European Union Horizon Europe programme under Grant Agreement No. 101217315. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.