Embedded System Management using WBEM

Michael Hutter, Alexander Szekely, Johannes Wolkerstorfer

IM 2009

Institute for Applied Information Processing and Communications (IAIK),
Graz University of Technology

About us

IAIK TU Graz

Graz University of Technology →
Faculty of Computer Science →
Institute for Applied Information Processing and Communications (IAIK)

Research groups

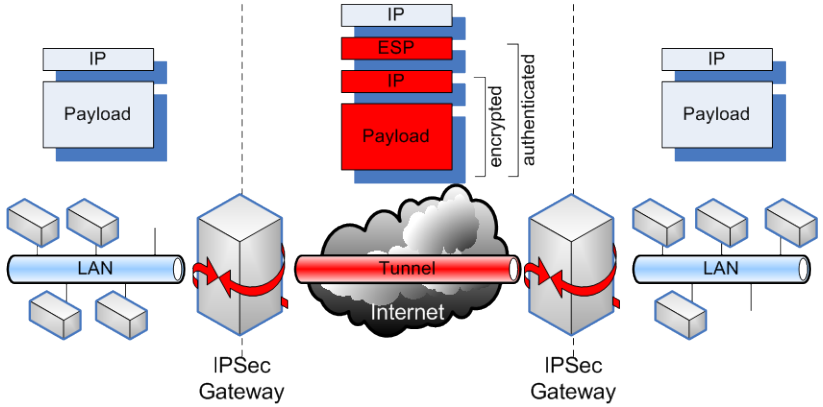
- Krypto group – Vincent Rijmen
- EGIZ (e-government)
- Trusted computing/Java security
- Network security
- Formal methods for design&verification
- VLSI group

Presentation Outline

- Introduction
  - Quantum Cryptography on Chip
- Embedded System Management
- Web-based Enterprise Management
  - Common Information Model
  - WBEM/CIM Server Requirements
- Our Implementation
  - Management Requirements
  - Implemented CIM Providers
  - Indications and Error Handling
  - CIM Client - Management Interface
- Performance Evaluation
- Conclusions

Introduction

- Quantum Cryptography on Chip (QCC) project
  - Austrian government and EU founded project (~500k€)
  - Partners: TU Graz, Siemens, Austrian Research Center (ARC)
- Implementation of an embedded IPsec gateway
  - Encrypt network traffic on layer 3
  - Gigabit throughput
  - Key exchange using quantum cryptography



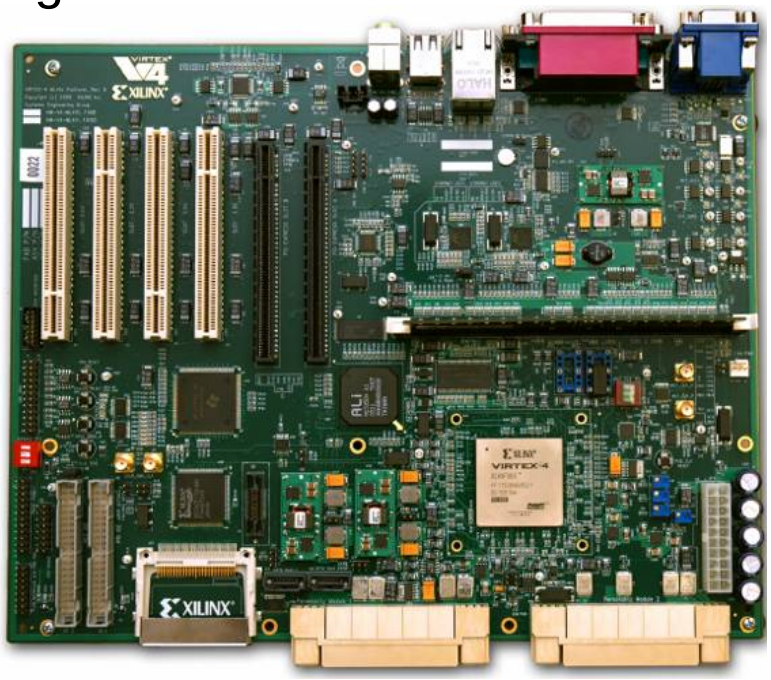
- Management of embedded IPsec gateways

Quantum Cryptography on Chip

- Classical cryptography combined with quantum key exchange
- Keys are provided by a quantum channel
  - Quantum optical setup (fibre-optic channel)
  - Key distillation from entangled photons
- Embedded IPsec gateway composed of several parts
  - IPsec module (AES encryption/decryption)
  - Quantum Data Acquisition (QDAQ) unit
  - Quantum Key Distribution (QKD) unit
  - Quantum Internet Key Exchange (QIKE) unit

Embedded System Platform

- Xilinx ML410 board used as prototyping board
- Virtex-4 FX60 FPGA
  - Configurable logic blocks
- PowerPC-405 32-bit CPU
- 2 Ethernet MAC/PHY (Gigabit)
- Compact Flash
  - For system configuration
  - File system for Linux
- Other features
  - DDR2, Flash, SouthBridge, VGA, Audio, PCI bus, USB, UART, LCD, ...

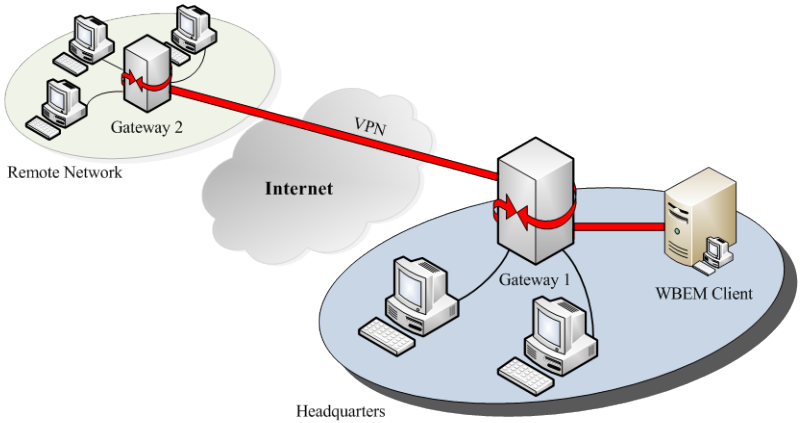


- How to manage this device?

ML410 board © Xilinx

Embedded System Management

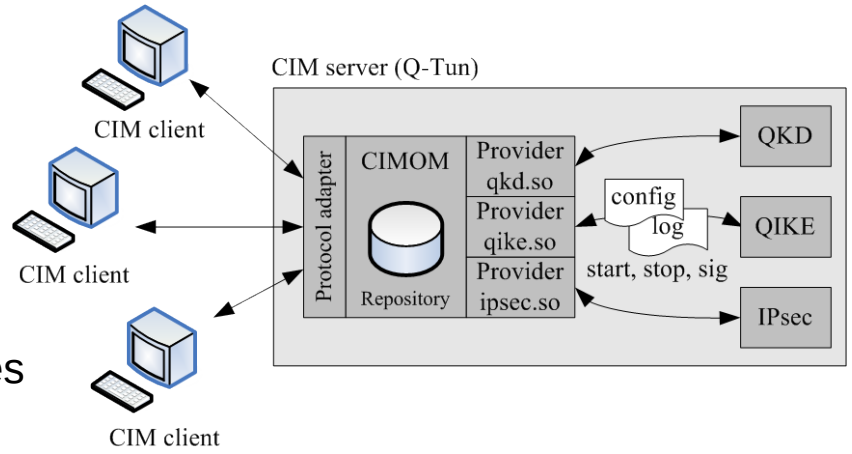
- Resource-constrained environments
  - Less memory available
  - Low processing power
  - Low power/battery lifetime
- How to manage heterogeneous networks?
  - Multiple vendors
  - Different software (operating systems,…)
  - Different hardware (CPUs, hard disks, …)
  - E.g. cell phones, domestic appliances, embedded IP routers
- Different management solutions
  - Command Line Interface, remote shell, SNMP, CMIP
  - Web-based solutions (tiny Web servers)
    - SOAP
    - UDDI
    - WSDL
    - Netconf
    - JMX
    - Web-based Enterprise Management (WBEM)
- What is WBEM and is it suitable for embedded devices?



Web-Based Enterprise Management

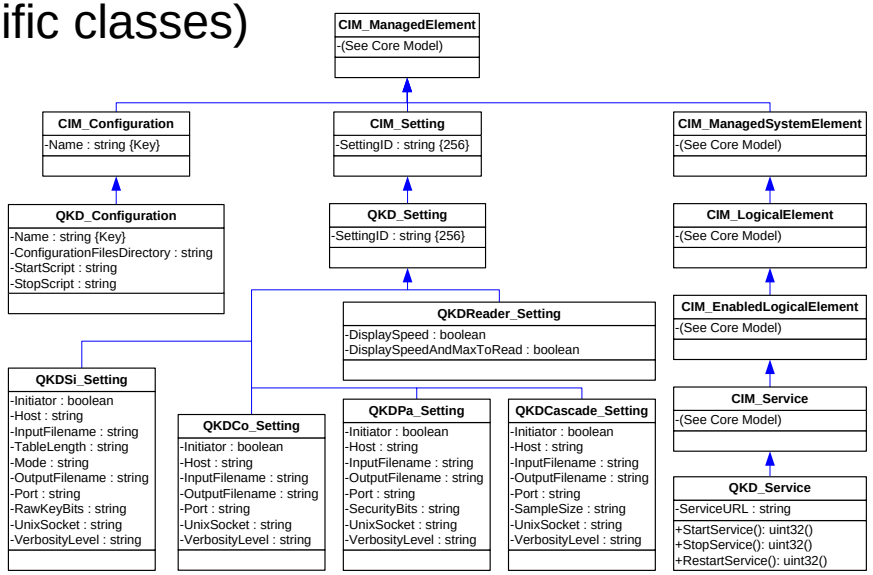
- Set of Internet standards and standards from the Distributed Management Task Force (DMTF)
  - Aims to solve the problems of interoperability
    - Common standards (data exchange, modeling, interfaces …)
  - Aims to solve the problems of expandability
    - Object-oriented model supporting inheritance

- WBEM system architecture
  - Client interface
  - WBEM/CIM server (object manager)
  - Providers used to access the resources



Common Information Model

- Model that describes the management data
  - Model description (CIM schema) provided by DMTF
- Model Hierarchy
  - Core model (essential classes)
  - Common model (technology specific classes)
  - Extension model (application specific classes)
- Extension of the model
  - Managed Object Format (MOF)
  - Registration to the server



WBEM/CIM Server Requirements

- Focused on open source and C supporting servers
- Performance Metric
  - Static and dynamic memory consumption in kB (after startup, after 10x enumerateInstance operation)
  - Test platform: dual-core PC (2.8 GHz, 1GB memory)
  - 32-bit Ubuntu Linux
  - All WBEM/CIM implementations hold the same number of CIM classes

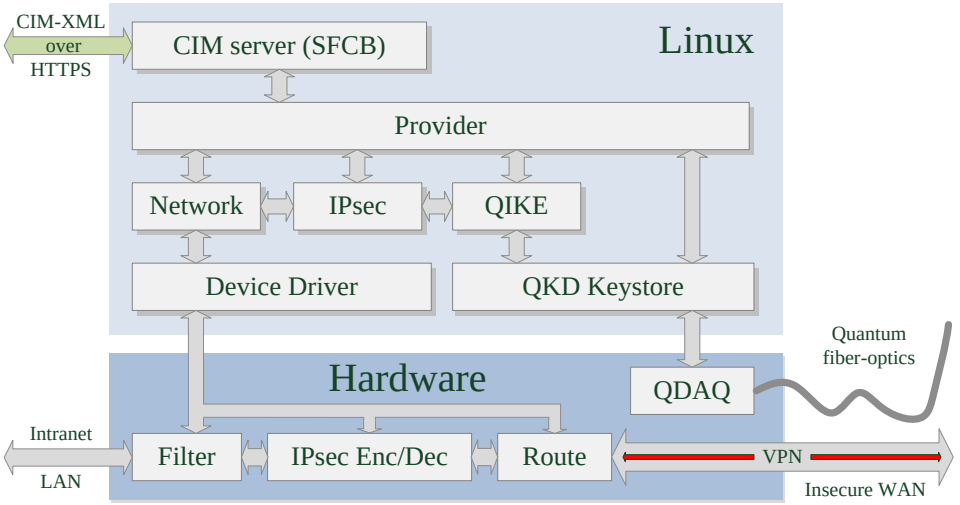
	openWBEM		openPegasus		SFCB	
	After startup	**After enumInst**	**After startup**	**After enumInst**	**After startup**	**After enumInst**
Total RSS	4496	5388	5328	13468	1896	2728
Private RSS	3668	4440	4484	10492	792	1612
Shared RSS	828	948	844	2976	1104	1116
Effective RSS	3956	4756	4756	12836	1360	2192
Disk space	50900		9800		1900	

Small Footprint CIM Broker (SFCB)

- Open source project
- CIM Object Manager (CIMOM)
- Written in C
- Especially designed for resource-constrained environments
- Features
  - Secure Socket Layer (SSL)
  - Service Location Protocol (SLP)
  - Stable: provider segfault does not bring down the CIMOM
- CMPI Support, CIM-XML, MOF, CIM providers
- HTTP chunking
- Indications for event handling
- Binary repository

Management Requirements

- Management of different resources
  - Configuration of network settings (IP routing tables, …)
  - IPsec policies
  - QKD settings
  - QIKE
  - Operating system status
  - Command control
- Error handling and monitoring
  - Recovery of settings after reboot
  - Display of QKD error rate
  - Display of QKD data rate
  - System status/warnings
- Security
  - Authentication of the client
  - Communication with embedded devices over a secure tunnel



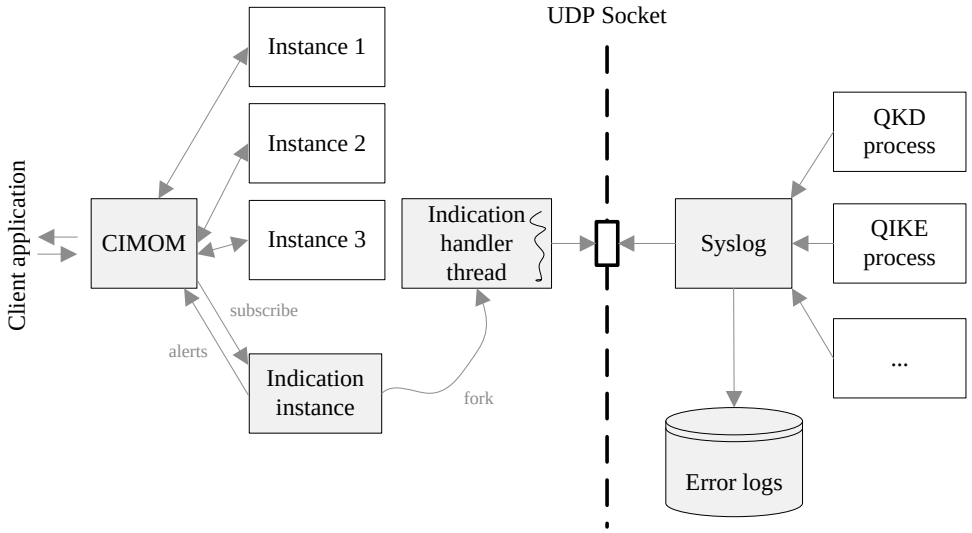
CIM Providers

- Translate CIM formatted requests of the CIMOM to the specific operation of the managed resource
- 59 CIM providers located in six different provider libraries
- Extension of the CIM schema v2.9.0

	Instance	Association	Method	Indication
Network	17	9	3	0
IPsec	3	0	1	0
QKD	8	0	2	1
QIKE	17	0	1	1
OS	12	5	2	1
Syslog	2	1	0	0
Total	**59**	**15**	**9**	**3**

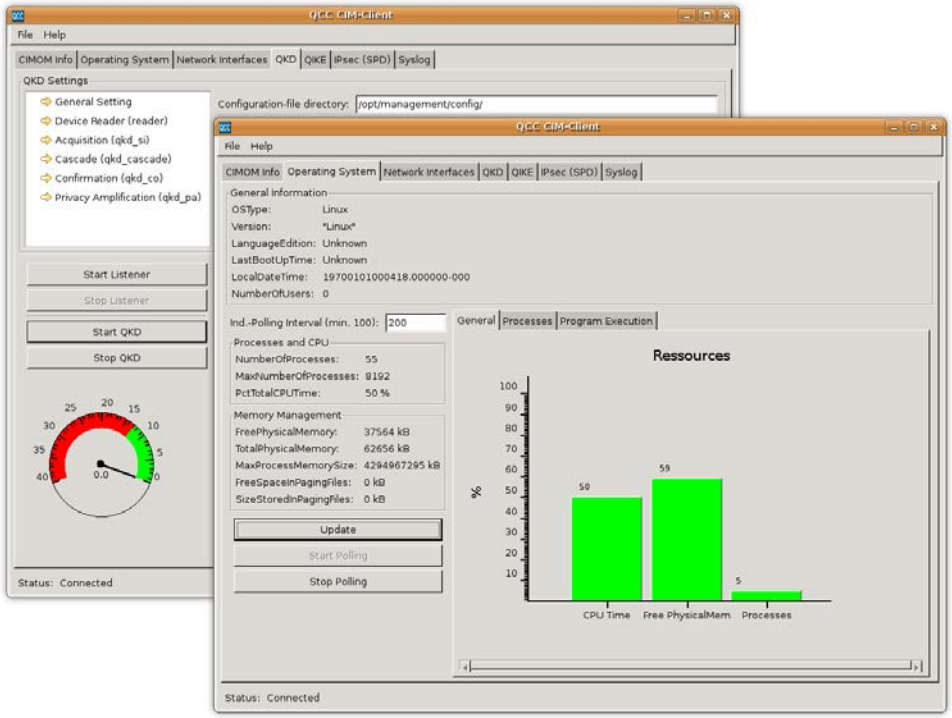
Indications and Error Handling

- All configuration data and settings are stored in files
  - Located in non-volatile memory
  - Recovery of settings after an (un)intended reboot
- Run-time errors are logged using Syslog
- Support of indications, e.g. error-rate monitoring



WBEM/CIM Client Interface

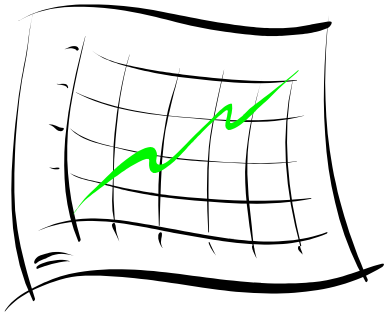
- Configuration
  - Network, IPsec, QKD settings, …
- Security Policies for IPsec gateways
- Command Control
  - Starting and stopping the QKD stack
- Display resources
  - Operating system status
- Monitoring/Alerts
  - Key data rates
  - Error rates



Performance Evaluation

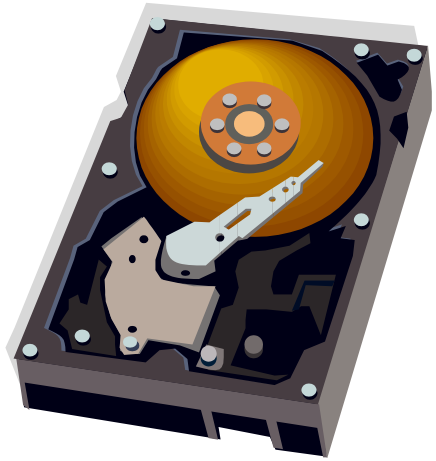
- Is WBEM/CIM realizable on embedded devices?
- How is the efficiency and performance?

- Evaluation of
  - Disk-space usage
  - Running time
  - CPU utilization



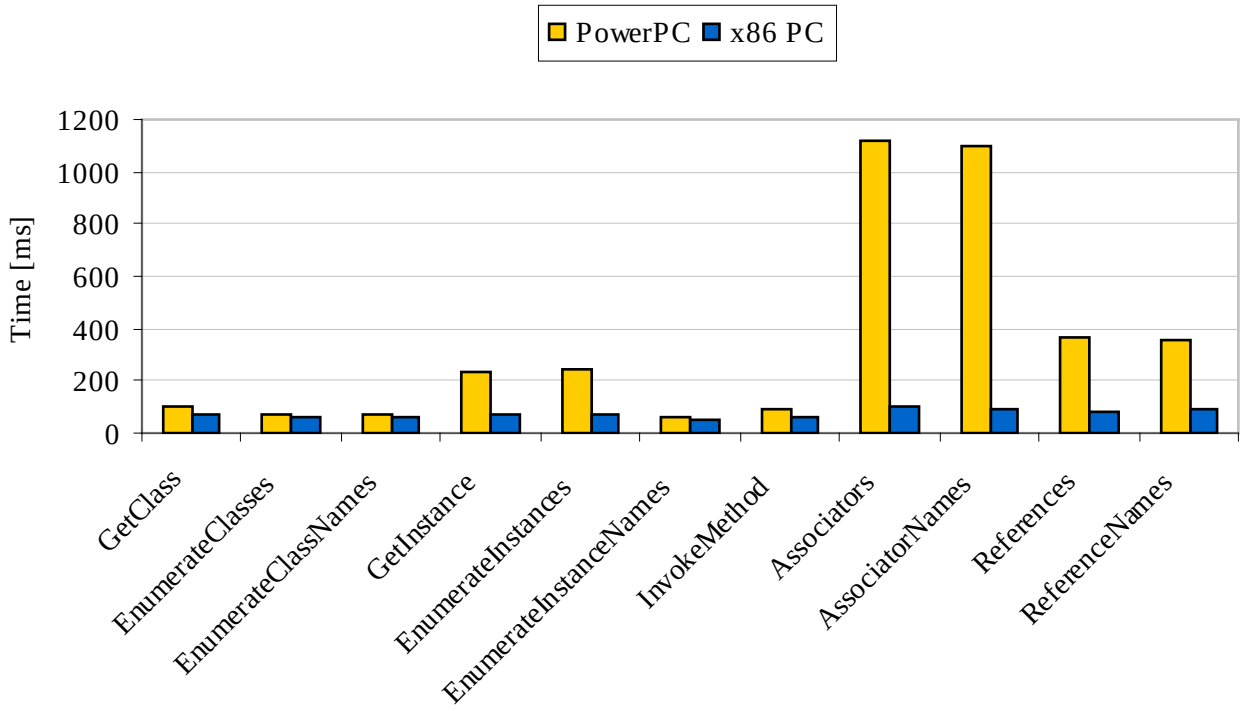
Disk-Space Usage

- Size of the SFCB server shrinked down to 899 kB
  - Caching and compressing data of repository
  - Compiler options (debug support, file optimization, …)
- Size of providers
  - Network: 312 kB
  - IPsec: 97 kB
  - QKD: 180 kB
  - QIKE: 368 kB
  - OS: 215 kB
  - Syslog: 30
  - **Total: 1202 kB**

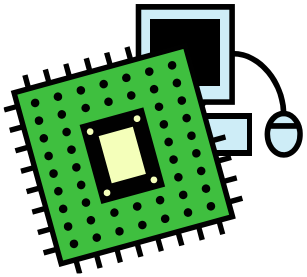


Run-Time Performance

- Running time of different CIM operations measured
- Comparison of embedded PowerPC vs. x86 PC



CPU-Time Profiling



- CPU load of different CIM operations measured

	PowerPC [%]			x86 PC [%]		
	user	**kernel**	**Idle**	**user**	**kernel**	**idle**
Idle	2	1	97	2	1	97
enumerateClasses	37	59	4	47	9	44
enumerateClassNames	40	34	26	48	7	45
enumerateInstances	27	65	8	49	9	42
enumerateInstanceNames	24	35	41	48	9	43
getClass	43	29	28	46	7	47
getInstance	25	66	9	49	8	43
invokeMethod	22	57	21	49	6	45
associators	35	62	3	42	15	43
associatorNames	36	61	3	41	13	46
references	43	52	5	45	14	41
referenceNames	41	53	6	44	13	43

- Bottleneck is not the WBEM/CIM processing

Conclusions

- Implementation of a quantum-enabled IPsec gateway that uses a light-weight WBEM/CIM architecture
- Secure management of resources of different gateways
- Fast response times, low memory footprint and CPU usage
- Easy interoperability and expandability
- But: higher resources are needed by providers to provide all interfaces (compared to proprietary solutions)
- Embedded WBEM/CIM proofed to be applicable in practice

Thanks for your attention!

Questions?

http://www.iaik.tugraz.at/