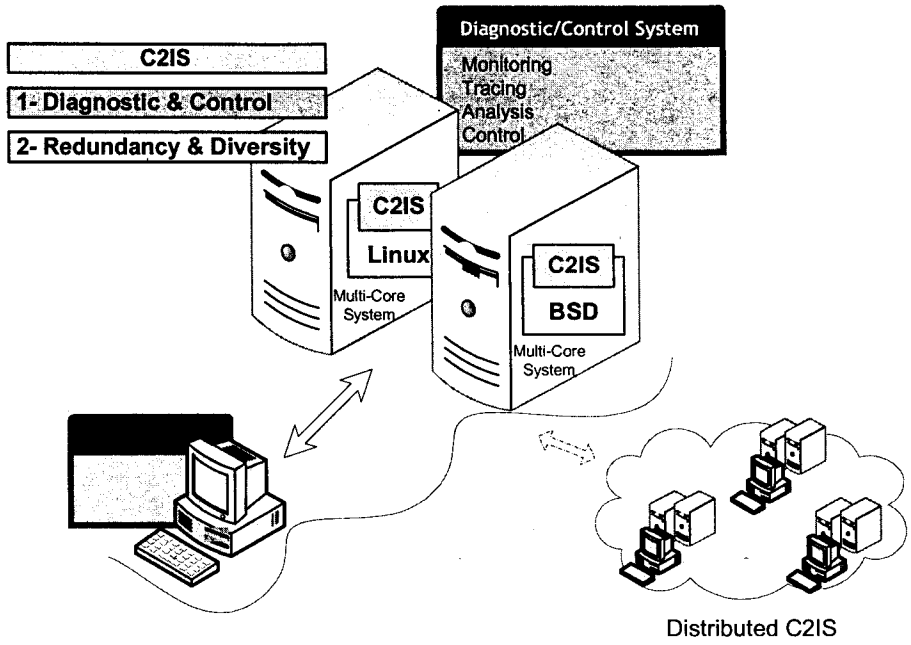
SL 2009-339 532733



15BA: Multi-core Monitoring and Soft Redundancy for Cyber Attack Resistance (Poly-Tracing)

Delivery by: DRDC Valcartier, SAR/SoS
Start-End: 2009-04 – 2012-03
Total Funds: 1923.6 k$ (all contributors)
Total FTE (DRDC): 5.4

PM: Mario Couture
Sponsor: Dir. Information Management Security [7]

Objectives:

1- Develop advanced capabilities for the surveillance and protection of C2 software apps executed in distributed multi-core multi-level env.;
2- Significantly improve cyber attack resistance and continuity of services in hostile environments through novel software architectures that involve the use of diversity and redundancy in critical infrastructures

Capability Deficiency/DND Project:

Command: Cyber attack vulnerabilities & system availability
Act: Non-kinetic effects
Shield: Force protection (limited detect./prot. against cyber threats)
DND Project: Pro-active Computer Network Defence (CND) / 266

ADM(S&T) Hard Problems:

HD5: Close Capability Gaps and provide Alternative Solutions identified within the CF Strategic Capability Roadmap
HD12: Enhance the nation's cyber security

Technologies:

C2IS, Diagnostic/corrective system, LTTng, Eclipse, *Linux*, Windows

Key Outputs:

1- *State of the art reports*: a) Monitoring/Tracing n-core CPUs [1]; b) Hybrid redundant architectures (updated twice)
2- *Feasibility studies*: a) Monitoring/Tracing n-core CPUs [2]; b) Hybrid redundant architectures (updated twice during ARP)
3- *Soft. modules & techniques*: a) Linux Tracing Toolkit (LTTng) (FOSS); b) Advanced techniques for hybrid redundant architectures
4- *Demonstrations*: a) Advanced capabilities for surveillance, analysis & control of n-core distributed systems; b) Hybrid redundant arch.

Key Outcomes:

1- Advanced capabilities (incl. soft. tools & techniques) for the online semi-assisted surveillance & protection of distributed complex C2ISs
2- Improved deep investigation capabilities
3- Redundancy extensions for attack resistance, resiliency & maintenance

Revised 25-Mar-2009 by B. Wong / É. Bossé

Multi-core Monitoring and Soft Redundancy for Cyber Attack Resistance; 15BA

Milestones/Planned Completion Date /Actual Completion Date:

1- 15BA05 started: April 09

- 15BA05: 10 milestones [6]
- 6 SOTAs updated (15BA05): Sept. 09/Nov. 09

2- Workshop on software redundancy & diversity: Fall 09

- 1 SOTA redundancy (15BA02): Feb. 10/Feb. 10
- 1 SOTA resilience (15BA05): Feb. 10/Feb. 10
- 15BA05: 1 milestone
- 15BA02: 1 milestone

3- Mid-project evaluation – 15BA05: Fall 10

- 15BA05: 17 milestones [6]
- 15BA02: 1 milestones

4- Mid-project evaluation – 15BA02: Spring 11

- 15BA05: 9 milestones [6]

5- Demonstration: 15BA05: Spring 11

6- Demonstration: 15BA02: Autumn 12

- 15BA05: 21 milestones [6]
- 15BA02: 2 milestones

SOTA: State of the art
OS: Operating system

Progress:

Work done:

1- SOTA (v1.0): Monitoring/Tracing of multi-core systems [1, 3]
2- Feasibility studies: [2]
3- Tutorial Monitoring/Tracing of multi-core systems [4]
4- Kickoff (15BA05): April 9th 2009
5- Tracing Mini-Summit 2009: Montreal, July 14th 2009
6- Global project review & brainstorming: Sept. 09

On-going/next work:

7- Update 6 SOTAs (one per R&D thread) [6]: Nov. 09
8- DRDC contract definition: Resilience (begin Sept. 09)
9- One Post Doc: Redundancy diversity (begin Jul. 09)
10- SOTAs Meeting: Dec. 2009, Montréal

Risks/Issues:

1- NSERC approval of joint project [6] (solved)
2- Convergence of industrial and governmental priorities (solved)
3- **S&T**: Each of the 6 main R&D threads of 15BA05 [6]
4- **S&T**: Definition of the theoretical framework for redundancy
5- **S&T**: Fine cyber attack resistance, resilience and quick recovery

Project team:

M. Couture (DS): 80%
R. Charpentier (DS): 70%
D. Thibault (CS): 30%

Technology readiness levels:

Start: between 2 & 3
End: between 6 & 7

15BA – The 3 Main S&T Threads and Clients

Current client:
Dir. Information Management Security

Poly-Tracing project ➔

Deep monitoring, tracing, analysis of n-core n-level distributed information systems
(3-to-1 leveraging project)
(15BA05)

Software redundancy and diversity
(Post Doc)
(15BA02)

Software resilience, self-adaptation, self-healing
(DRDC contracts)
(15BA05)

Next generation R&D/S&T projects
(15BA06; Agility)

Resources (15BA)

(k$)	08/09 (Prel. studies)	09/10 (Year 1)	10/11 (Year 2)	11/12 (Year 3)
15BA05 (Poly-Tracing)	80 + 11.5	120	120	40 - 80
15BA02 (Redundancy)	-	40	90	90
15BA06 (Agility)		35		
FTE equiv. DRDC	90	170	170	170
Total DRDC contrib.	91.5 + 90 = **181.5**	195 + 170 = **365**	210 + 170 = **380**	130 + 170 = **300**
Total DRDC contrib.	**1 226.5**			
15BA03 NSERC	25	79.5	79.5 + 75	79.5
15BA04 Ericsson	40	64.4 + 75 + In kind (16.8)	64.4 + In kind (16.8)	64.4 + In kind (16.8)
Total Ext. contrib.	**65**	**235.7**	**235.7**	**160.7**
Total All contrib.	**1 923.6**			

DRDC

External

Current situation

C2ISs are (and will continue to be) made of increasingly complex technologies (softw./hardw.)
- Multi-proc., multi-core, multi-level (virtualization), geographically distributed, etc.

C2ISs are often utilized in hostile and constrained environments
- Network (Internet), rough & constrained physical spaces (mil. platforms), etc.

Current limitations:
It is now *impossible* to build fully certified C2ISs (*we must learn to live with software defects*)
C2ISs are harder to debug, optimize and adapt to new demanding situations
C2ISs are subject to serious cyber threats (*current security frameworks are not sufficient*)
It is often very hard to detect and eliminate unwanted internal software behaviours during Ops
- They result from cyber attacks, design faults, operator errors and other kinds of threats

New complementary technologies are needed during operations for:
The deep monitoring, tracing and fine analysis/control of C2ISs
The protection of C2ISs against unwanted software behaviours
The improvement of officers' situation awareness (C2ISs' current states)

Competitors: to our knowledge, there is no competitor to this project
Only the LTTng tool has the necessary very low overhead on ISs and OSs at runtime
LTTng is part of the mainline of the Linux kernel; *maintained at Mtl Polytechnique*
Poly-Tracing project brings together some of the best Canadian researchers:
- The kernel of OSs, the complexity of software and hardware technologies
- Trace abstraction & analysis, corrective measures identification/application

(Directly)/(indirectly) involved major industries: *(Ericsson, Red Hat)/(IBM, Google)*

C2ISs: Command and Control Information Systems

Expected Innovation

The Vision

Online fine surveillance & protection of distributed complex C2ISs
- This technology will be "complementary" to the current security framework

Continually updated easy & quick to understand awareness of the health of C2ISs
- "Zoomable" pictures of C2ISs' states of health
- "Zoomable" pictures describing detected problems & available solution options

Improved protection of C2ISs against unwanted software behaviours during operations

Easy/quick to implement solution options to solve detected problems during operations
- Increased flexibility and rapidity of action
- Choice among well pre-studied solution options (and probable impacts)
- Reconfiguration mechanisms (redundancy & diversity)
- Pro-active mechanisms for software resilience, self-adaptation and self-healing

The ability to save data for deep cyber forensics post-analyses (conducted in-lab)

New technologies to be utilized *during operations* and for *deep in-lab analyses*

➔ *A Feedback-directed semi-assisted diagnostic/corrective system for C2ISs*

➔ *A framework allowing improved utilization of redundancy & diversity in architectures*

C2ISs: Command and Control Information Systems

References

[1] Couture *et al.*, 2008a. *Monitoring and Tracing of Critical Software Systems - SOTA*, DRDC Valcartier TM 2008-144, June 2008.

[2] Couture *et al.*, 2008b. Tracing, *Monitoring and Analysis of distributed Multi-core Information Systems - Selected Feasibility Studies*, DRDC Valcartier TR 2008-300, November 2008.

[3] Dagenais *et al.*, 2008a. *State-Of-The-Art Tracing and Monitoring Multicore Execution*, Polytechnique Montréal, November 2008.

[4] Dagenais *et al.*, 2008b. *State-Of-The-Art Tracing and Monitoring Multicore Execution.* Tutorial given at Bell Centre Ottawa on November 2008 to 25 key DND people

[5] Charpentier & Dagenais, 2008. *Rapport d'atelier stratégique CRSNG*, STPWS 364780-08, July 2008.

[6] Dagenais *et al.*, 2008c. *Tracing and Monitoring Tools for Distributed Multi-Core Systems*, NSERC 90429374, July 2008.

[7] LCol Jackson DIM Secur, 2008. *Support letter -Multicore Tracing Project*, February 2008.

[8] Heikkila & Gulliksen, 2007. *Multi-Core Computing in Embedded Applications*, VDC Market Research, September 2007.

[9] Kienzle *et al.*, 2007. *Survivable Service-Oriented Computing Systems for Hostile Environments*, McGill University, October 2007.