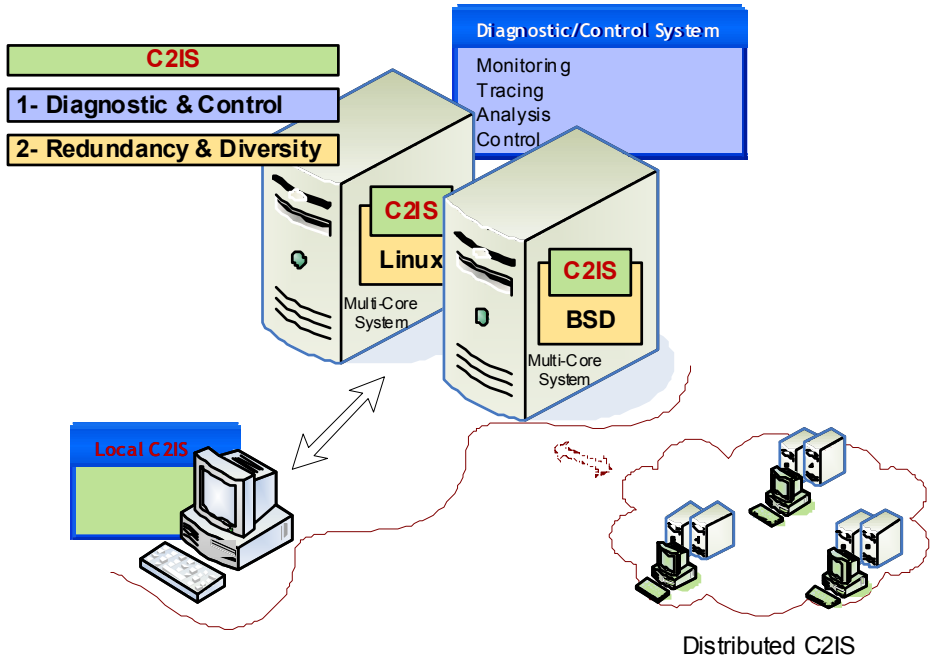
DEFENCE R&D DÉFENSE

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

PG 5A Command and Control
Thrust Advisory Group Meeting

Mario Couture
DRDC Valcartier / System of systems

May 12th, 2011



DEFENCE R&D DÉFENSE

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

Delivery by: DRDC Valcartier (SAR/SOS)
Start-End: 04/09 – 03/12
Total Funding: 2.9 M$
Total FTE: 5.4 (DRDC)
Sponsor: Dir. Information Management Security

PD: Mr. Paul Béland
PM: Mr. Mario Couture

Objectives: 1- *Develop advanced capabilities for the surveillance and protection of information systems* executed in distributed multi-core multi-level environments;
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 detection / protection 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: Command and control information systems and devices involving the Linux operating system (telephones, PDAs, etc.), advanced on-line surveillance systems, software tracing and trace analysis, Eclipse, Linux, Windows

Key Outputs:

1- *State of the art reports*: a) Monitoring/Tracing n-core CPUs; b) Hybrid redundant architectures (updated twice).

2- *Feasibility studies*: a) Monitoring/Tracing n-core CPUs; b) Hybrid redundant architectures (updated twice during ARP).

3- *Soft. modules & techniques*: a) Linux Tracing Toolkit (LTTng); b) Advanced techniques for hybrid redundant architectures.

4- *Demonstrations*: a) Advanced capabilities for surveillance, analysis & control of n-core distributed systems; b) Hybrid redundant architecture.

Key Outcomes:

1- Advanced capabilities (incl. software tools & techniques) for the on-line semi-assisted surveillance & protection of distributed complex C2ISs (multi-core, multi-level).

2- Improved deep investigation capabilities.

3- Redundancy and diversity extensions for attack resistance, resiliency & maintenance.

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

DEFENCE R&D DÉFENSE

Overall Status: Green

The 15BA project defines a technological basis that will allow the development of the next generation of surveillance systems for operational servers, laptops, cell phones, and the like, which will help duty officers build/maintain a host-based situation awareness (health states, detected anomalies, and possible courses of action).

Milestones (overview)	WBE	Compl.	Status
Preliminary studies/workshop	15BA05	Apr-09	Complete
Six SOTAs (+1; Ericsson) (+1; U.C.)	15BA05	Dec-09	Complete
SOTA (red.-div.) (Post Doc)	15BA02	Jul-09	Complete
Analysis/prototype (red.-div.) (U.C.)	15BA02	Mar-11	Complete
Techniques: trace abstraction/analysis	15BA05	Dec-10	Complete
SOTA/analysis security systems	15BA05	Jan-11	Complete
½-Project eval. (+ tutor./wkshp)	15BA05	Dec-10	Complete
½-Project eval. (+ tutor./wkshp) (2X)	15BA02	Mar-11	Complete
SOTA (models of the Linux kernel)	15BA05	Mar-11	Complete
Techniques (I) (7 R&D threads)	15BA05	Dec-11	Complete
Techniques: red.-div. (Lin.-BSD)	15BA02	Mar-12	On-going
Next S&T project preliminary studies	15BA07	Mar-12	On-going
Final developments	15BA05	Mar-12	On-going
Final developments	15BA02	Oct-12	On-going
End-project demonstration (devel.)	15BA05	Apr-12	Started
End-project demonstration (devel.)	15BA02	Nov-12	Started
Publication of results + closing report	15BA05	Mar-12	On-going
Publication of results + closing report	15BA02	Nov-12	On-going

Progress:

Work done (10/11):

-New techniques (15BA02, 15BA05) were developed and integrated in Eclipse
-Web site: Doc. + Demos->http://dmct.dorsal.polymtl.ca
-2 Mid-project evaluation meetings and Tutorials/workshops (15BA02, 15BA05)
-1 NSERC Strategic workshop (May 9-10th, Montreal)
-Three DRDC contracts (3 complementary studies)
-Publications (thesis/papers/reports)

On-going/next work (11/12):

-15BA02 + 15BA05 refinement of techniques, final developments, publications
-2 or 3 DRDC contracts (complementary studies)
-Develop the end-project demos (started)
-End-project demonstrations (15BA02 + 15BA05)
-Define the next DRDC project (ARP)
-Propose the new ARP to this TAG (Sept. 2011)

Risks/Issues:

A new Post-Doc: R. Khoury May-11 (solved; /contract)
Convergence of industrial and govt. priorities (solved)

Project team (DRDC Valcartier):

M. Couture (DS): 80%; R. Charpentier (DS): 20%; D. Thibault (CS): 80%

Technology readiness levels:

Start: between 2 & 3; End: between 5 & 6

Resources (15BA)

	(k$)	08/09 (Prel. studies)	09/10 (Year 1)	10/11 (Year 2)	11/12 (Year 3)
DRDC	**15BA05** (Poly-Tracing)	80 **+ 11.5**	120	120	40 + 80
DRDC	**15BA02** (Redundancy)	-	40	90 **+ 120**	90
DRDC	**15BA06/07** (Agility)			**+25 + 100**	
DRDC	FTE equiv. DRDC	**90**	170	170	170
DRDC	**DRDC contribution**	91.5 + 90 = **181.5**	195 + 170 = **330**	455 + 170 = **625**	130 + 170 = **300**
DRDC	**Total DRDC contribution**	**1,436.5**			
Partners	**15BA03** (NSERC)	**25**	79.5	79.5 + **46**	79.5 + **46**
Partners	**15BA04** (Ericsson)	**40** **+ In-kind**	64.4 + **75** + In-kind (41.4 + **121.6**)	64.4 + **75** + In-kind (41.4 +**207**)	64.4 + **75** + In-kind (41.4 + **207**)
Partners	**External contribution**	**65**	**~382**	**~513**	**~513**
	Total contribution	**2,909.5**			

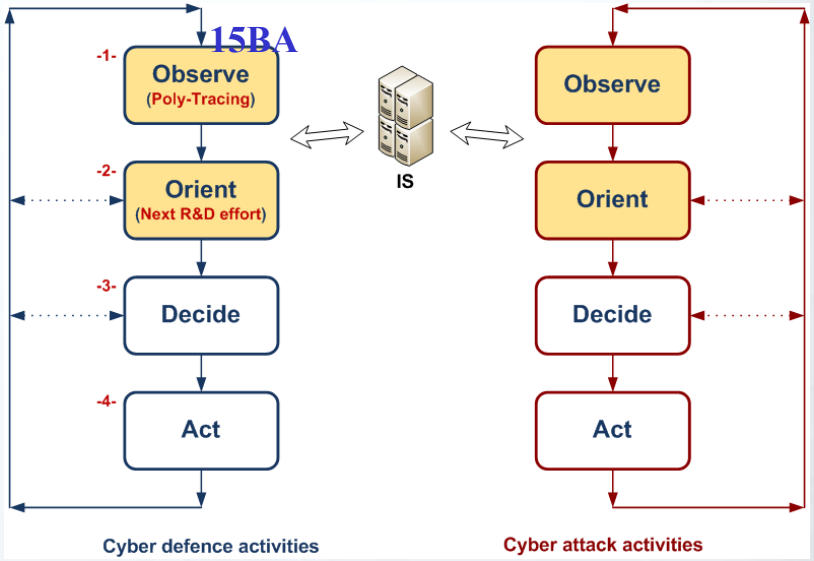
Red numbers represent additional supports to the project

Cyber surveillance of information systems

In the case of cyber warfare:

Cyber warfare involves two well-organised entities:
DND and ***bad (malicious) hackers***

OODA Loop as applied to ***host surveillance***:
-*Observe*: observation deep within the IS
-*Orient*: fast/advanced analysis, adapted reporting
-*Decide*: automatic/manual decision making
-*Act*: automatic/manual reactions and pro-actions



Some important technological needs:
-Better advanced techniques and models:
-for adaptive *observation* of hosts
-for adaptive *data abstraction, fusion, analysis*
-to *lower the number of false positives*
-Better *reporting* of:
-IS's health states
-detected undesired behaviours, states (*anomalies*)
-Suggest the *best courses of actions*

-The smallest overall "delta-t" (for the whole "blue" OODA Loop)

DND activities

Bad hackers activities

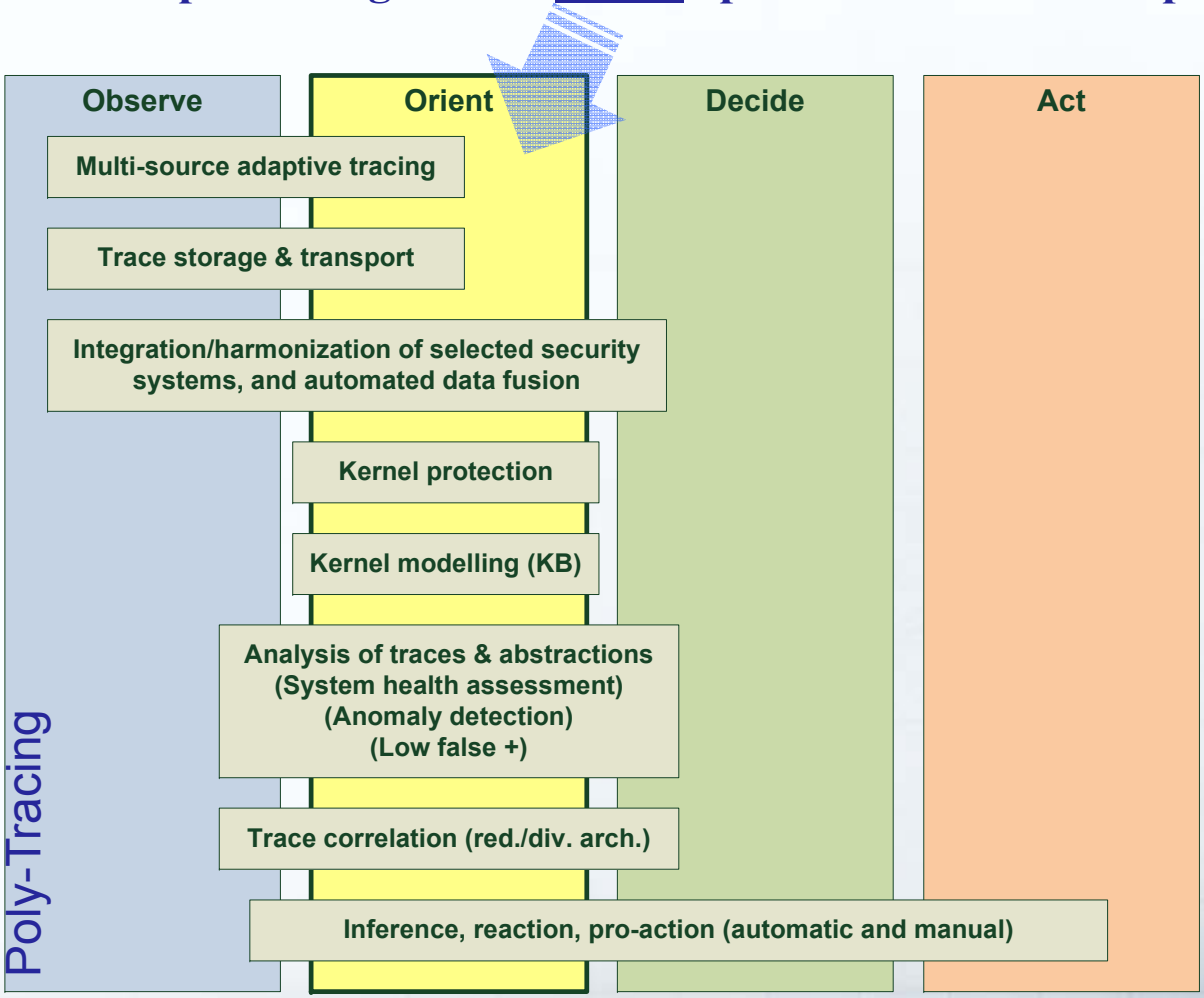
-Well organised
-Easy access to advanced hacking technology
-(…)

OODA: Observe, Orient, Decide, Act
DND: Department of national defence

Next DRDC project ("Orient")

Based on results obtained in the Poly-Tracing project, push further R&D efforts to:

improve significantly the efficiency & timeliness of activities pertaining to the "*Orient*" part of the OODA loop



To be submitted Sept. 2011