DEFENCE R&D DÉFENSE

Defence Research and Development Canada

The Poly-Tracing Project

DRDC Perspective

Mario Couture
Defence R&D Canada (DRDC Valcartier)

December 9th, 2011

Contents

1. My mandate at DRDC
2. DRDC concern: Online surveillance of ISs
3. Current project: Poly-Tracing – “Observe”
4. Next project – “Orient”
5. Concluding remarks

IS: Information system SoS: System of systems
VAL: Valcartier SRA: Software analysis and resilience

My Mandate at DRDC

1. **Capture and understand DND's technological needs and problems**
   - Create DRDC-DND workshops, meetings
   - Participate in DND working groups (national & international)
2. **Inform**
   - Preliminary studies (state-of-the-art, feasibility)
   - DRDC tutorials-workshops involving international experts (~2 per year)
3. **Initiate R&D and S&T efforts that will address problems**
   - Define National collaborative 3-year projects (DND-NSERC, MITACS)
   - Define DRDC contracts (2 or 3 per year) & in-house R&D & S&T, prototyping
   - Publications (national/international reports, scientific papers, presentations)

IS: Information system SoS: System of systems
VAL: Valcartier SRA: Software analysis and resilience

NSERC: Natural Sciences and Engineering Research Council of Canada
MITACS: http://www.mitacs.ca/

DRDC Concern: Online Surveillance of ISs

DEFENCE R&D DÉFENSE

Important facts:

1. Critical national infrastructures involve the use of *increasingly complex ISs*
2. Fielded ISs will always contain *unresolved design flaws* that will result in *errors/failures*
3. Malicious hackers are now very well *organised/sponsored* and have easy access to advanced hacking technologies (most of the time it is very cheap)
4. The ability of current surveillance systems (AV, HIDS, …) to detect undesired software states and behaviours within hosts *is dramatically limited*: **~30%** [Bell, 2010]

- The design of the **next generation of online surveillance systems** is a hard problem to solve
- DRDC has started to find and develop solution options (...)

AV: Antivirus HIDS: Host intrusion detection system IS: Information system

DRDC Concern: Online Surveillance of ISs

In the specific case of **cyber warfare**

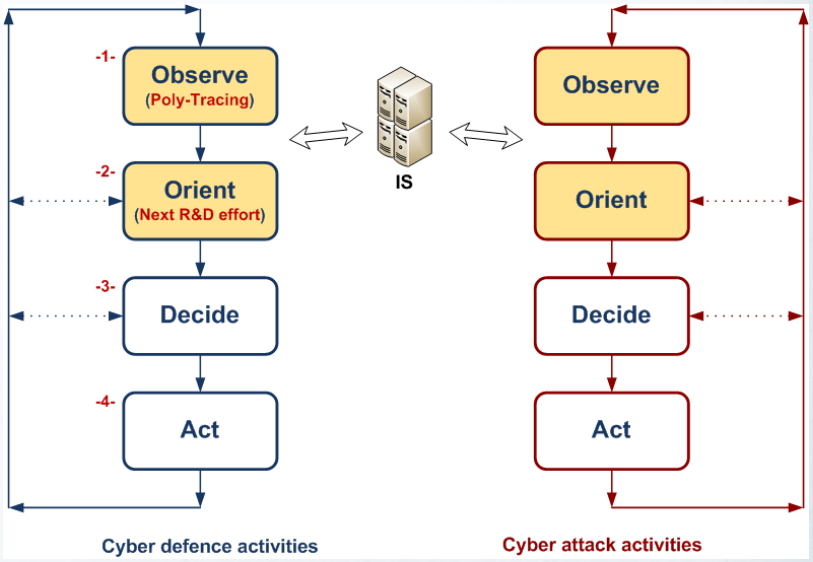
Two groups of people are involved:
Canadian Forces and **malicious hackers**

Def: ***OODA*** *Loop* as applied to *online host surveillance*:
-***O****bserve*: observation anywhere/anytime within an IS
-***O****rient*: detection analysis, low false positives, reporting
-***D****ecide*: automatic/human-assisted decision making
-***A****ct*: automatic/human-assisted reactions/pro-actions

➔The current project (addresses "Observe")
-Online *deep adaptive observation* of ISs
-New highly efficient *software tracing tool; LTTng*
-New techniques for *online trace analysis*

➔Next DRDC project (will address "Orient")
-Online *analysis* of observations (traces, events, ...)
-Improved *host-based situational awareness*

-*Adaptive resilience of ISs* (based on detected anomalies)



DND activities (CND/CNE/CNA)

Bad hackers activities

-Hackers are well organised
-Easy access to advanced hacking technology
-(…)

Ultimate goal: Improve the efficiency and timeliness of the whole **blue OODA Loop**

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

Current Project: Poly-Tracing – "Observe"

- Adaptive monitoring
- Trace events synchronization
- Trace events abstraction
- Automated fault identification
- Health monitoring and corrective measures
- Model-based instrumentation
- Impact inference
- Redundancy and diversity for security purposes

Mechanisms for source code instrumentation

LTTng tracer

Synchronization mechanisms

Language for fault ID

Abstraction mechanism and library

Mechanisms for impact prediction

Mechanisms for saving on disk behaviours, and replay the "history"

Reporting mechanisms

Control mechanisms

IS: Information system US: User space KS: Kernel space

The Next Project – "Orient"

DEFENCE R&D DÉFENSE

Title:

Online Surveillance of Critical IS through Advanced Host-based Detection

Main goals:

1-Online detection of *all kinds* of anomalies in IS with *low* false positives

2-Interoperability of host-based surveillance systems with network-level surveillance systems

3-Online capture of data for further offline analysis (forensic investigations, software improvement)

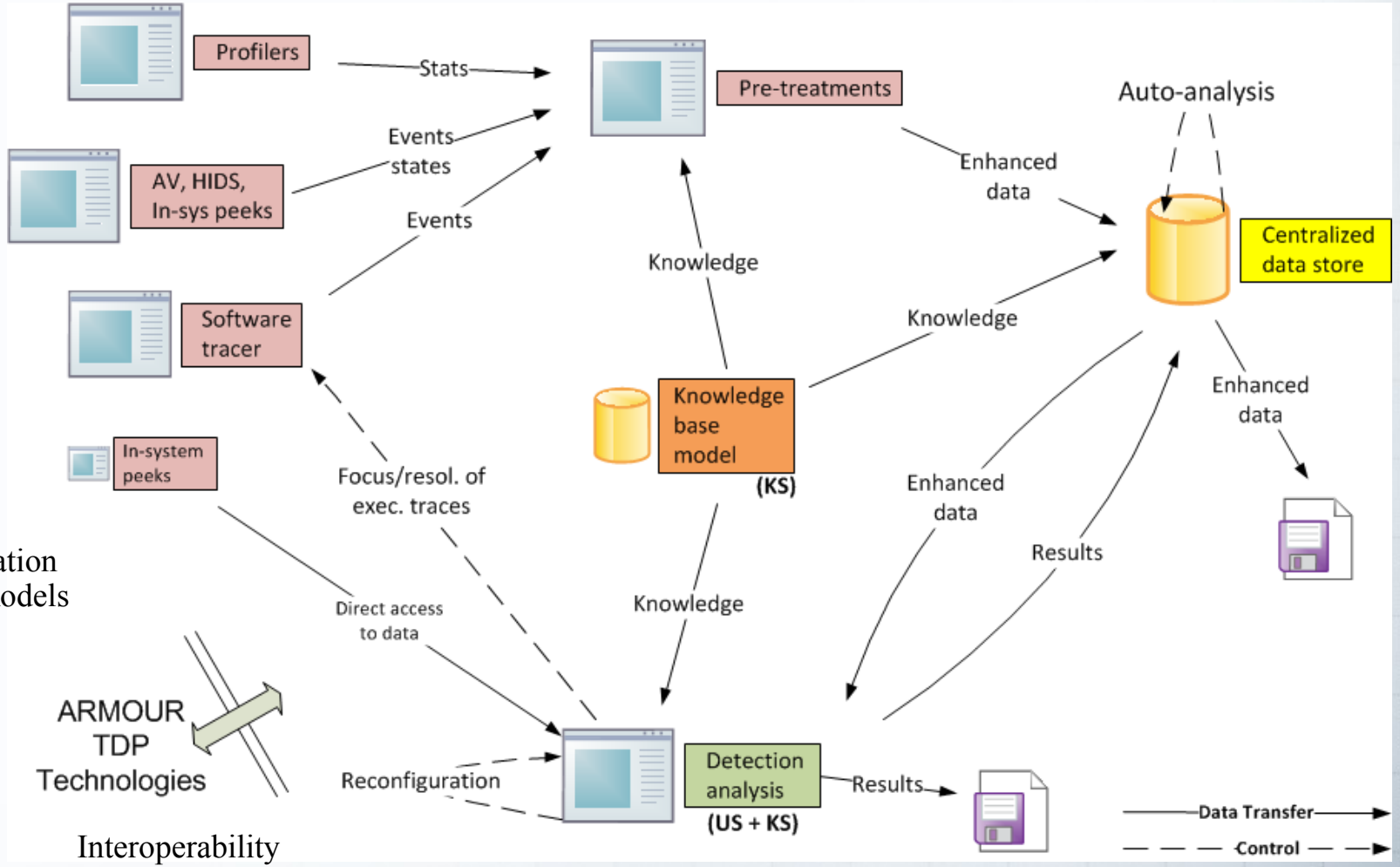
Emphasis will be put on the first item (the *hardest* problem to solve):

Very efficient online anomaly detection (with low false positives) in the context of critical intense military operations

IS: Information system

The Next Project – "Orient"

Online Feedback-Directed Surveillance Infrastructure – The Big Picture



Plus: Software instrumentation based on models

Interoperability

AV: Antivirus HIDS: Host intrusion detection system KS: kernel space, US: user space

The Next Project – Preliminary Studies

DEFENCE R&D DÉFENSE

Finalized DRDC contracts & PostDoc:

-Concordia U.: *Software resilience, self-healing, and self-adaptation*

-Concordia U.: *Cyber attack detection using redundant-diverse architectures*

-EfficiOS Inc.: *Knowledge base model for the Linux kernel*

-Revolution Linux: *Comprehensive analysis of Linux-based surveillance and security systems*

-DRDC: *Redundancy and diversity in software architecture for security purposes*

Ongoing DRDC contracts & PostDoc:

-Revolution Linux, DRDC: *Analysis of Linux-based security systems outputs for data fusion purposes*

-U. of Toronto: *A comprehensive analysis of kernel exploits for the Linux operating system*

-DRDC: *Redundancy and diversity in architectures for highly resilient information systems*

-DRDC, Concordia U.: *Adaptive resilience for ISs*

IS: Information system

The Next Project – Preliminary Studies

Supplementary tasks were added to the Poly-Tracing project:

-U. Laval: *Software behaviour models for the detection of anomalies*

-Concordia U.: *Taxonomy of Linux kernel-level attack types*

-Concordia U.:

- -*Operating system health states*
- -*New anomaly detection techniques*
- -*The lowering of false positives*
- -*Other studies*

-Montreal Polytechnique:

- -Implementation of LTTng *in the user space of* a:
  - -BSD-like operating system and
  - -MS-like operating system

Concluding Remarks (I)

ALL: please update our web site with your work **(http://dmct.dorsal.polymtl.ca/):**

-A brief description of all the *technologies* that you are (will be) developing

-Upload all the technologies/data/documentation/(...) (under Projects or Tools??)

-A well identified section (in each Project) for the technologies (under projects or Tools?)

-*Publications*

-Upload a copy of all related publications (pdf)

-*Demos*

-Please upload your demos/data/documentation/(how-to)

-If possible: already installed in a virtual machine (adapted for non-experts)

-A well identified section (in each project) for the demos

-*Tools* (all tools?), *Events* (all types of past, current and future events?, pictures?)

➔Please Yannick, we need your help for these tasks

IS: Information system US: User space KS: Kernel space

Concluding Remarks (II)

-Keep in mind the big picture:

-*Complex debugging* of multi-core ISs is very important

-Integrate Poly-Tracing technologies in the TMF framework

-This may take time if you don't have the "how-to" and if you start from zero

-Please ask Yannick for help (he will ease and accelerate this task)

-***Online deep surveillance* of ISs is very important as well**

-Observation (*Poly-Tracing*): *adaptive efficient tracing of IS*

-Orient (*next project*): *anomaly detection* with *low false positive rates*

-Decide and Act (*future project*): *adaptive resilience* for IS

-Again, please update our web site with your latest documents, files, (...)

-This will help people from DRDC and DND understand all this work (some are non-experts)

-All the work that is done in this project is recognized as valuable to DND

IS: Information system

Mario.Couture@DRDC-RDDC.GC.CA
DRDC Valcartier
(418) 844-4000 (4285)

http://lttng.org/

http://dmct.dorsal.polymtl.ca

http://www.eclipse.org/linuxtools/