DEFENCE R&D DÉFENSE

Defence Research and Development Canada

Cyber surveillance of information systems

Technological problems and needs

Mario Couture
Defence R&D Canada (DRDC Valcartier)

Partnership workshop
Montreal Polytechnique

May 9-10th, 2011

Content

1. Definitions and domain of work
2. Important facts
3. Cyber surveillance of information systems
4. Current project: Poly-Tracing (“Observe”)
5. Next project: (“Orient”)
6. Concluding remarks

Definitions and domain of work

Information system (IS):

- A "computerised system" allowing the *processing and sharing* of data and information
  - With this *generic definition*, a cell phone can be considered as an IS

Surveillance of ISs:

- The use of specialised software systems (AV, HIDS, software tracers, etc.) for the *observation* and *analysis* of ISs' states and behaviours
- *On-line surveillance* during operations, automatic/manual, locally/remotely controlled
- Detect and report appropriately ***any undesired anomalies*** (with ***low false positives***)
- Focus on the health of the IS: expected system performances and responses, no undesired behaviours/states at all levels (US, KS)

Domain of work:

- *DRDC Valcartier* ➔ ***host surveillance***
- DRDC Ottawa ➔ network surveillance

} Collaborative work

AV: Antivirus
HIDS: Host intrusion detection system
US: User space
KS: Kernel space

Important facts

Some important facts [Charpentier & Lefebvre, 2010]**:**

- Critical national infrastructures involve the use of increasingly *complex ISs*
- Fielded ISs will *always* contain unresolved design flaws & bugs (potential vulnerabilities)
- Nowadays malicious hackers are very well organised/sponsored and they have easy access to advanced hacking technologies (which are often cheap)
- The ability of current surveillance systems (AV, HIDS, …) to detect undesired software states and behaviours within hosts *is dramatically limited: ~30%* [Bell, 2010].

The development of the next generation of surveillance systems is not an easy to solve problem. This is why

- *sustained iterative and incremental collaborative R&D efforts are needed*

The current and future projects described today are examples of such efforts

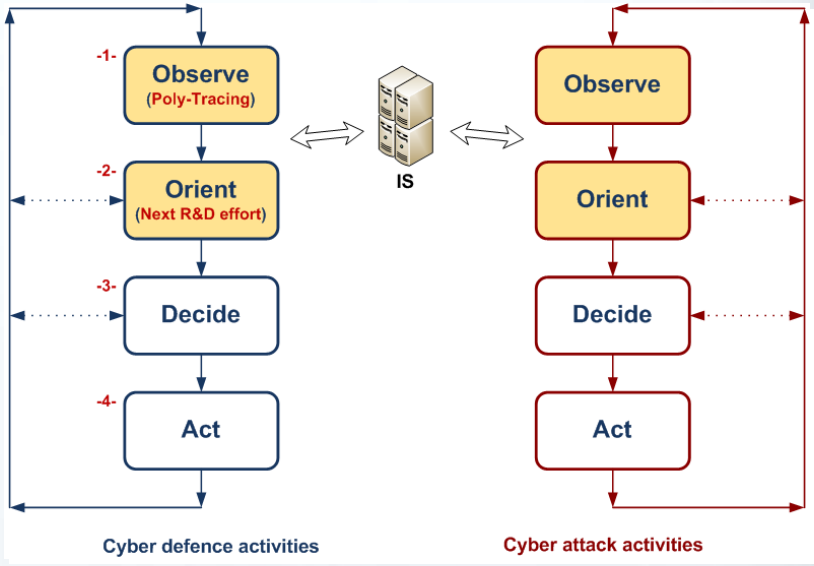
AV: Antivirus
HIDS: Host intrusion detection system
IS: Information system

Cyber surveillance of information systems

In the case of cyber warfare:

Cyber warfare involves two well organised entities:
DND and ***bad 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



DND activities

Bad hackers activities

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)

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

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

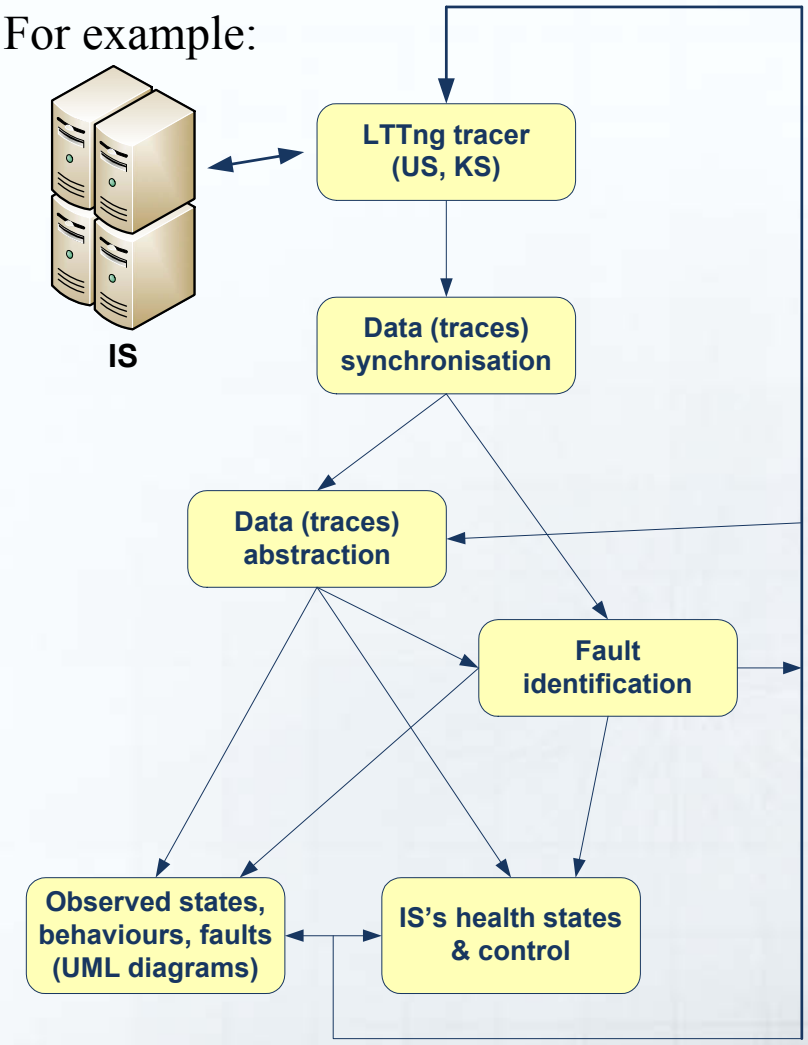
Current project: Poly-Tracing ("Observe")

DEFENCE R&D DÉFENSE

Main R&D threads
(Poly-Tracing project)

- Automatic/manual deep monitoring of ISs
- Data synchronisation
- Data abstraction
- Automated fault identification
- Health monitoring and corrective measures
- Trace directed modelling
- Impacts prediction (of monitoring)
- Redundancy and diversity for security purposes

For example:



Feedback-directed

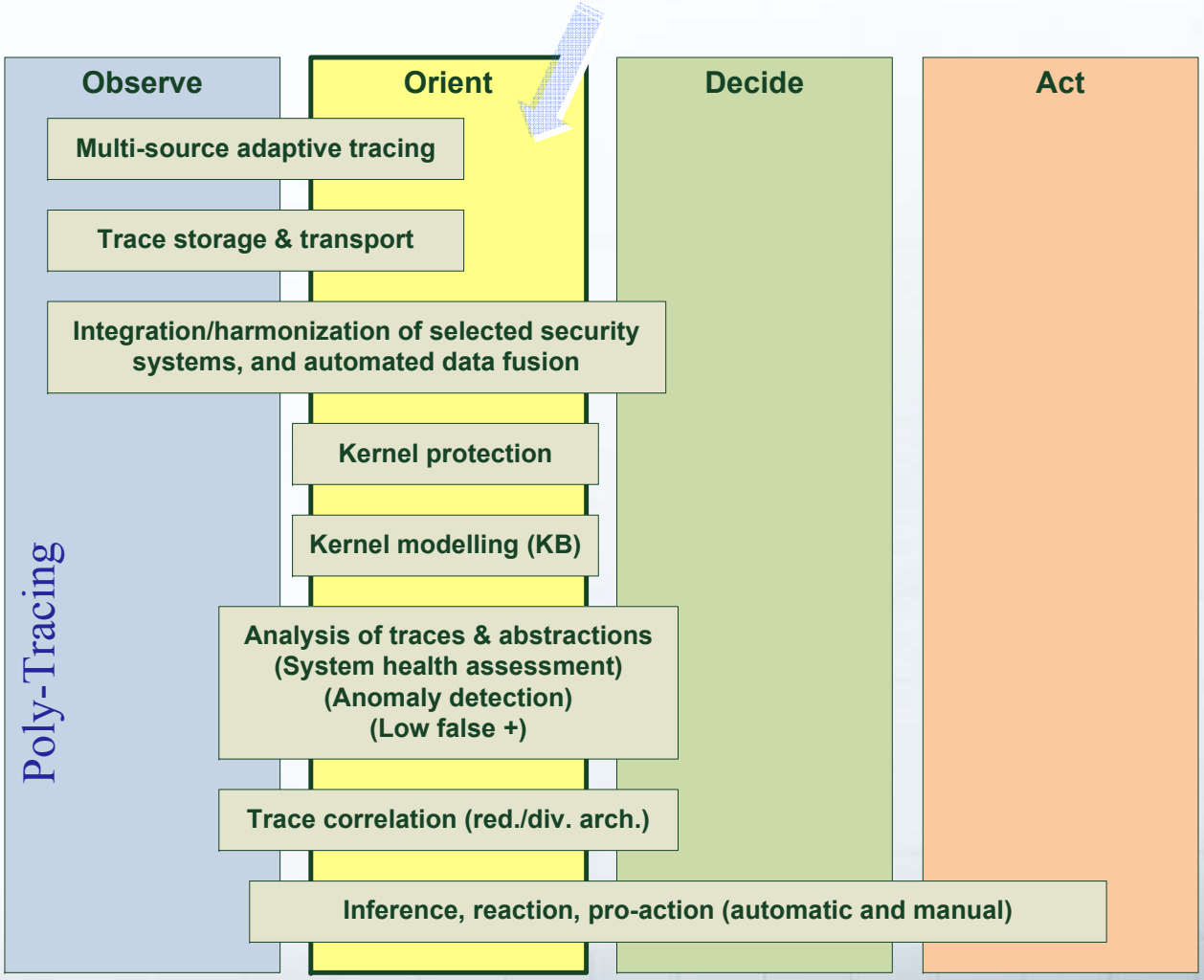
Documentation & demos:
(http://dmct.dorsal.polymtl.ca)

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

Next 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



Concluding remarks (I)

Poly-Tracing project (the on-going project):

Type: 4-year DND-NSERC project (2.6 M$)

Partners:

Ericsson Canada, NSERC, DRDC Valcartier

4 Cdn univ.: 5 PhDs, more than 15 grad. students

Open source: developed technologies are (and will continue to be) developed/improved by other experts from government, industry, and academic organisations

DND: Department of national defence
NSERC: Natural Sciences and Engineering Research Council of Canada

Concluding remarks (II)

Next project (to be submitted September 2011):

Type: DND-NSERC project (strong interest: academic and industrial organisations)

Size: similar to the Poly-Tracing project

DND: Department of national defence
NSERC: Natural Sciences and Engineering Research Council of Canada

Open source has proved to be a very good approach

Ultimate goals of the next project:

Detect and report *all kinds of anomalies* in ISs (malicious/non-malicious, *low false* +)

Help operators on duty *build and maintain a full HSA* of their ISs during operations

This is not an easy problem ➔ collaborative iterative & incremental R&D efforts

The main goals of this workshop:

Discuss important technological problems/needs (*host level surveillance*)

Identify R&D topics that should be addressed in the next project

Explore possible research partnerships

HSA: Host-based situation awareness
IS: Information system

DEFENCE R&D DÉFENSE

Contact:

Mario Couture, Defence scientist

DRDC Valcartier

Mario.Couture@DRDC-RDDC.GC.CA

(418) 844-4000 4285