DEFENCE R&D DÉFENSE

Defence Research and Development Canada

Cyber surveillance of information systems

Current and future DRDC projects

Mario Couture
DRDC Valcartier (SoS/SAR)

February 2011

Content

1. Surveillance of information systems
2. Current DRDC efforts – “Observe”
3. Next DRDC efforts – “Orient”
4. Concluding remarks

Surveillance of information systems

IS: a computerized "system" allowing the processing and sharing of data, information, and knowledge

Domains of work:

- DRDC Valcartier (SoS) ➔ *surveillance of hosts*
- DRDC Ottawa (NIO) ➔ surveillance of networks

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 black-hat hackers are very well organised & they have easy access to advanced technologies
- The ability of current surveillance systems (AV, HIDS, …) to detect undesired software states and behaviours is dramatically limited: ~30% [Bell, 2010]. *This is a serious problem*

Many "hard problems" must be addressed to improve the "dependability" of ISs during operations

➔Sustained major iterative & incremental collaborative R&D efforts are needed←

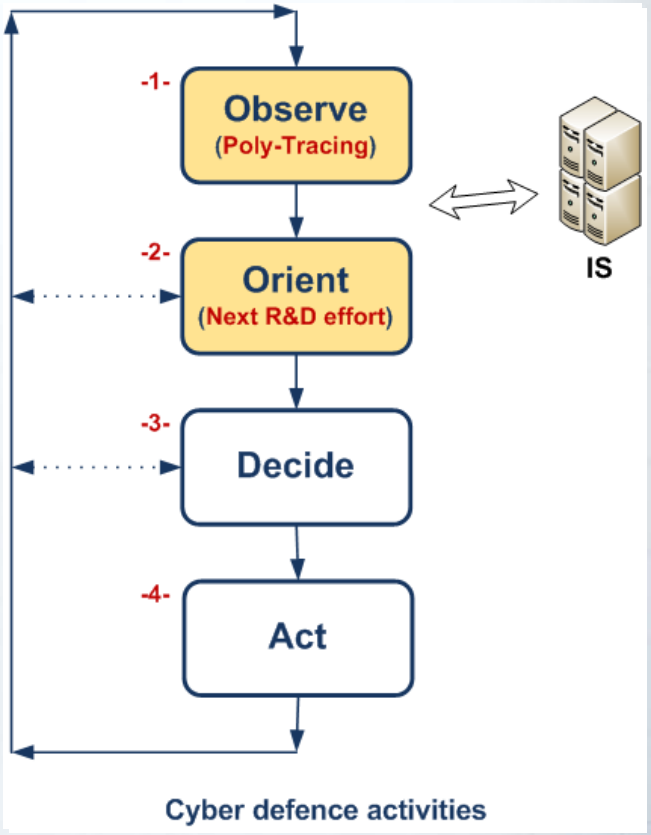
The DRDC projects described in this presentation are examples of such efforts for DND

AV: Antivirus
HIDS: Host intrusion detection system
IS: Information system
COA: course of actions

Surveillance of information systems

OODA Loop; in the case of host surveillance:

-Observe: deep monitoring
-Orient: very fast advanced analysis, adapted reporting
-Decide: automatic/manual decision processes
-Act: automatic/manual reactions and pro-actions



Some important needs:

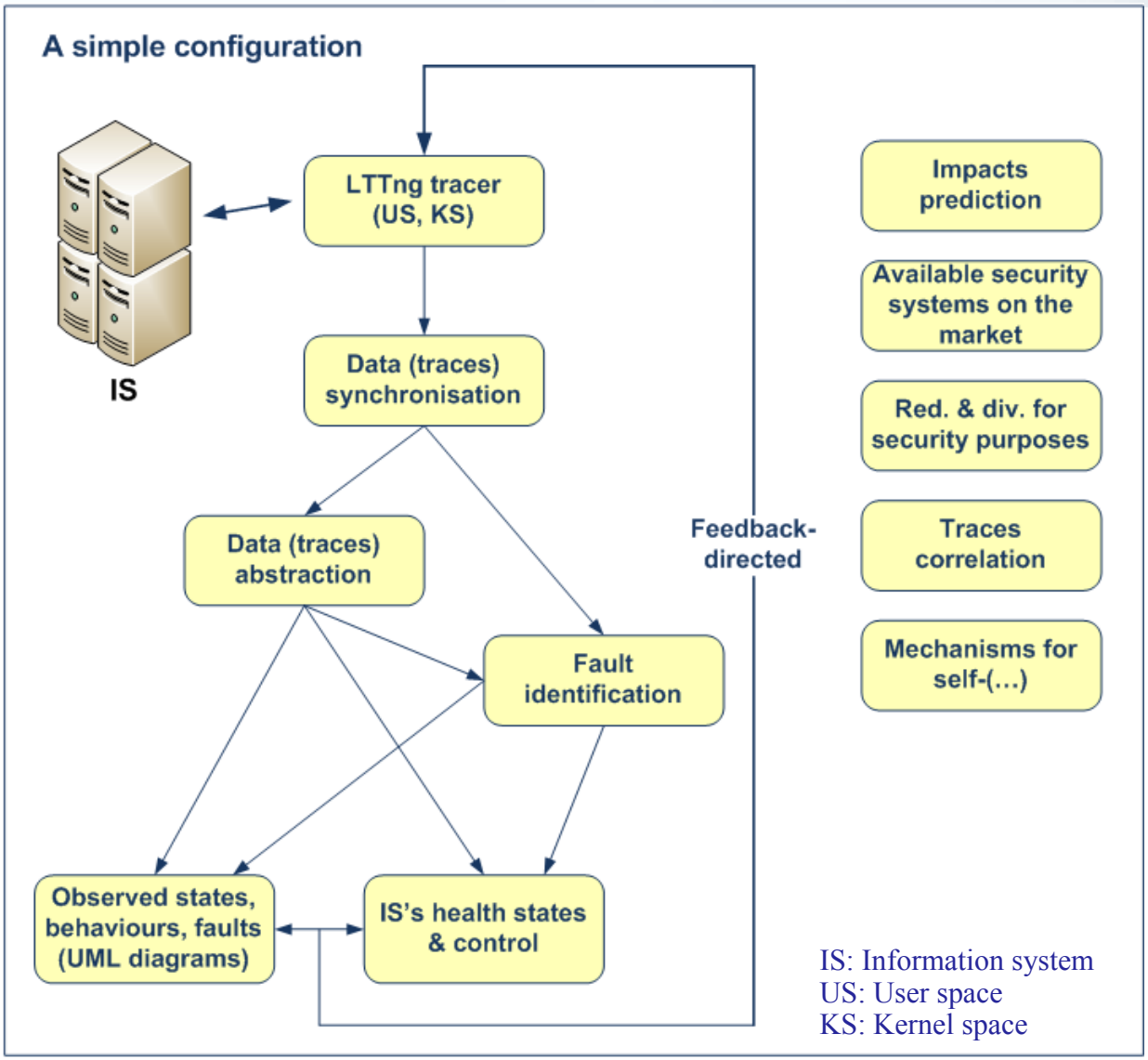
-Better mechanisms:
  -for adaptive observation of hosts
  -for adaptive data abstraction, fusion, analysis
  -to lower the number of false positives
-Better reporting of:
  -IS's health states
  -detected undesired behaviours, states, anomalies
-Propose officers on duty the best courses of actions
-Very small overall "delta-t" (of the whole OODA Loop)

OODA: Observe, Orient, Decide, Act
IS: Information system
HSA: Host-based situation awareness

Current DRDC efforts – “Observe”

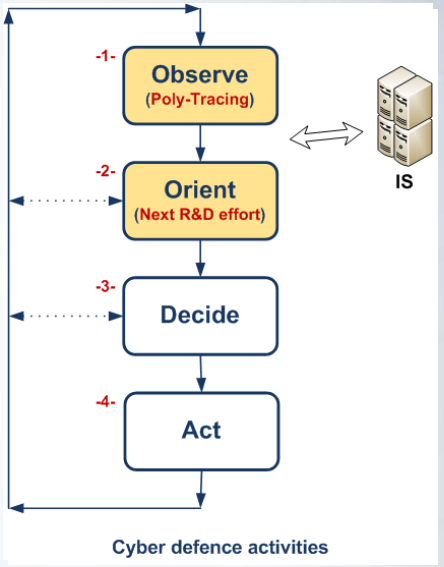
R&D threads in the Poly-Tracing project (“Observe”)

- 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
- Security systems currently available on the market



Self-(…): resilience, self-adaptation, self-healing, …

Next DRDC efforts – "Orient"



Based on Poly-Tracing results, push further R&D efforts to:

➔**Improve significantly "Orient"-related activities**←

Some important needs:

- **Consider the evolution of *IS's health states* during operations**
- **Consider *all kinds of anomalies* in the IS (not limited to "known malware")**
- New highly-efficient models and techniques for:
  - Quasi real-time analyses, alarms management, elimination of false positives
  - Automatic/manual reactive and pro-active COAs
  - The resilience, self-adaptation, and self-healing of ISs (i.e. red. & div. in arch.)
- Integrate available efficient surveillance systems (AV, HIDS, …) from the market
- **Help officers on duty build and maintain a HSA of their ISs during operations**
- **Full interoperability with network surveillance systems (push/pull modes)**

➔**The next DRDC project is currently under definition**←

AV: Antivirus
HIDS: Host intrusion detection system
HSA: Host-based situation awareness
COA: Course of actions
IS: Information system

Concluding remarks

Poly-Tracing & redundancy-diversity (on-going):

- A 3-year DND-NSERC project; 2.6 M$
- 3 partners: DRDC, Ericsson, NSERC
- 5 PhDs, more than 15 graduate students, Post-Docs
- Post-Docs at Valcartier, many DRDC contracts

Preliminary studies for the next DRDC project

- Additional 220 k$ (financial support: DRDC)

Next DRDC projects (will be submitted in September 2011):

- Type: DND-NSERC project (academic and industrial orgs are already involved)
- Size: similar to Poly-Tracing

DEFENCE R&D DÉFENSE

This technology is Open source

It is (will be made) available @:

http://lttng.org/

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

Next event

On-line cyber surveillance of information systems

Presentations of results and way-ahead

-Tutorial (4 presentations will be given by 3 experts)

-Workshop (capture DND's technical problems & needs)

Ottawa; March 8th, 2011

(The number of available seats is limited (~2), please contact M. Couture to reserve one)

Mario.Couture@DRDC-RDDC.GC.CA

(418) 844-4000 (4285)

Backup Slide