On-line cyber surveillance of information systems

Results from the current DRDC project, and way-ahead

March 8th, 2011

Bell Communications Centre
(Theatre Room)
160 Elgin Street - 14th Floor
Ottawa, Canada

In recent years, the Internet and cellular networks have become the centre of most interactions, from text, voice and video applications to shopping, entertainment, information gathering and, importantly, government services and operations. The newer electronic service centres are now built out as clusters of numerous high-performances, relatively low-cost multi-core computers connected through redundant high-speed networks. Furthermore, these clusters are efficiently shared among several different applications which need peak resources at different times. In such a context, where services are offered in the cloud, it becomes extremely difficult to *monitor and optimize the performance and security of each service*.

The development and deployment of the next-generation on-line surveillance infrastructure involves the iterative and incremental solving of complex conceptual and technical problems through major R&D/S&T collaborative projects that involve the active participation of academic, industrial and governmental organisations. The *DRDC Poly-Tracing Project* is one of these. Already, in its first two years, it has shown that low overhead on-line adaptive tracing/monitoring/analysis techniques have the potential to bridge current and future technological gaps in this important domain. On-line deep surveillance of redundant-diverse critical information systems can significantly contribute to reducing the risks of security problems, detecting and blocking intrusions very early in the contamination process, surviving, and avoiding the extreme costs of long-lasting undetected anomalies in systems (be they caused by malicious activities or not).

This meeting aims to:

a) **inform attendees on recent technical advances made in the Poly-Tracing Project;**
b) **examine the way-ahead (0 to 5 years); and**
c) **discuss the relevance of various technological options.**

The meeting is intended for managers and technical staff involved in cyber security, information system optimization, and complex development and debugging. It is unclassified and free. As the number of seats is limited, interested parties should reply quickly **by e-mail** to Mario Couture and mention their **name/organisation/e-mail**.

Mario Couture
Mario.Couture@drdc-rddc.gc.ca
418-844-4000 (4285)

Agenda

8h30-8h45: Introduction (M. Couture)

8h45-9h30: Defending software against the 2011 cyber threat (R. Charpentier)

Present the DRDC technical strategy for developing a permanent cyber force within the Canadian Forces, based on the proactive defence concept. The presentation will include an introduction to cyber attacks, an update on the cyber threat as observed in Canada in 2011, and an overview of some initiatives to improve the protection of our infrastructures.

9h30-10h00: Discussion

10h00-10h30: Coffee break

10h30-11h30: Redundancy and diversity in architectures for cyber protection – A critical review (A. Hamou-Lhadj)

Present the state of the art and preliminary results of the last DRDC experimentations involving trace correlations in the context of redundant-diverse architectures for cyber surveillance. Make recommendations for future studies, developments and experimentations.

11h30-12h00: Discussion

12h00-13h00: Lunch

13h00-14h00: Results from the Poly-Tracing Project, and way-ahead – Part 1 (M. Dagenais)

This research has produced a low-level, low-overhead tracing and monitoring framework. Extremely efficient algorithms for the surveillance of information systems, scalable to many-core distributed architectures, have been designed and implemented. The resulting software modules attracted collaborators from numerous major companies besides Ericsson (IBM, Google, Fujitsu, Red Hat, and Novell) and are used around the world. The presentation will describe each of these elements and explain how these modules can be used in the context of cyber surveillance. A description of needed R&D efforts will also be presented.

14h00-14h30: Discussion

14h30-15h00: Coffee break

15h00-16h00: Results from the Poly-Tracing Project, and way-ahead – Part 2 (A. Hamou-Lhadj)

Advanced techniques were developed to transform the observed low-level data into meaningful and manageable information (rendered as high-level software behavioural patterns). Further research must be done to adapt these techniques to on-line cyber surveillance. The presentation will describe the results obtained so far. Some aspects of future research will also be described (such as advanced techniques and reference models for quasi real-time data abstraction and analysis).

16h00-17h00: Discussion

17h00: End of the meeting

Biographies

Dr. Michel Dagenais

Michel Dagenais is a professor at École Polytechnique, Montreal, Canada, in the Computer and Software Engineering Department. He has been active in the area of system analysis tools for the past 15 years. He has over the years visited and collaborated with researchers at many of the largest industrial research centres at AT&T Bell Labs, Bell-Northern Research, Sun, DEC, IBM, Ericsson and Google. He spent industrial leaves at Sun, DEC and Ericsson Research. As part of the Canadian Consortium for Software Engineering Research (CSER), he was a co-recipient of the 2000 NSERC Leo Derikx Synergy Award, for "an innovative model of long-lasting university-industry interaction in a pre-competitive realm that has benefited the general well-being of an industry". The Linux Trace Toolkit, developed under his supervision at École Polytechnique, is used throughout the world and has gained the cooperation of a large number of industrial contributors over the years such as Autodesk Media and Entertainment, Google, IBM, Monta Vista, Sony, and others.

Dr. Abdelwahab Hamou-Lhadj

Abdelwahab Hamou-Lhadj is an Assistant Professor in the Department of Electrical and Computer Engineering (ECE) at Concordia University, Montreal, Canada. He holds a Ph.D. degree in Computer Science from the University of Ottawa, Canada. He has been working for many years in the area of dynamic analysis of software systems with an emphasis on program comprehension. At Concordia, he leads a research group that investigates techniques and tools to help software engineers understand the behavioural aspects of large and complex software systems through the study of their execution traces. His research contributions resulted in many published articles that have been cited extensively in the literature. He is also the leader of an international workshop on the topic co-located with the prestigious Working Conference on Reverse Engineering (WCRE).

Mr. Robert Charpentier

Mr. Robert Charpentier completed his degree in engineering physics at "l'École Polytechnique de Montréal" in 1979. After working at CAE Electronics on flight simulators, he joined what was then Defence Research Establishment Valcartier (now DRDC Valcartier), where he specialised in infrared imagery and space-based surveillance. His current research domains are secure interoperability, automated software hardening, and software security design.

Mr. Mario Couture

Mr. Couture received a B.Sc. degree in Physics and an M.Sc. in Physical Oceanography at the Université du Québec à Rimouski, Qc, Canada. After 8 years of work in modelling and simulation at Fisheries and Ocean Canada, he completed an M.Sc. in Electrical Engineering at Laval University, Qc, Canada. In 2002, he joined Defence Research and Development Canada (DRDC Valcartier, Qc) as a Defence Scientist in the Software Analysis and Robustness Group. His research interests are mainly oriented toward the study and design of leading-edge mechanisms for refined on-line surveillance and protection of military information systems.