RICIS TECHNICAL NOTE

Integrity and Security in an Ada Runtime Environment

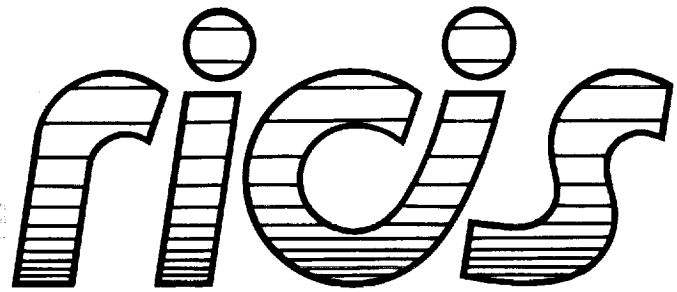
Rodney L. Bown

University of Houston-Clear Lake

June, 1991

Cooperative Agreement NCC 9-16
Research Activity No. SE.26

NASA Johnson Space Center
Engineering Directorate
Flight Data Systems Division



Research Institute for Computing and Information Systems
University of Houston - Clear Lake

T·E·C·H·N·I·C·A·L R·E·P·O·R·T

The RICIS Concept

The University of Houston-Clear Lake established the Research Institute for Computing and Information systems in 1986 to encourage NASA Johnson Space Center and local industry to actively support research in the computing and information sciences. As part of this endeavor, UH-Clear Lake proposed a partnership with JSC to jointly define and manage an integrated program of research in advanced data processing technology needed for JSC's main missions, including administrative, engineering and science responsibilities. JSC agreed and entered into a three-year cooperative agreement with UH-Clear Lake beginning in May, 1986, to jointly plan and execute such research through RICIS. Additionally, under Cooperative Agreement NCC 9-16, computing and educational facilities are shared by the two institutions to conduct the research.

The mission of RICIS is to conduct, coordinate and disseminate research on computing and information systems among researchers, sponsors and users from UH-Clear Lake, NASA/JSC, and other research organizations. Within UH-Clear Lake, the mission is being implemented through interdisciplinary involvement of faculty and students from each of the four schools: Business, Education, Human Sciences and Humanities, and Natural and Applied Sciences.

Other research organizations are involved via the "gateway" concept. UH-Clear Lake establishes relationships with other universities and research organizations, having common research interests, to provide additional sources of expertise to conduct needed research.

A major role of RICIS is to find the best match of sponsors, researchers and research objectives to advance knowledge in the computing and information sciences. Working jointly with NASA/JSC, RICIS advises on research needs, recommends principals for conducting the research, provides technical and administrative support to coordinate the research, and integrates technical results into the cooperative goals of UH-Clear Lake and NASA/JSC.

RICIS TECHNICAL NOTE

Integrity and Security in an Ada Runtime Environment

Preface

This research was conducted under auspices of the Research Institute for Computing and Information Systems by Dr. Rodney L. Bown, Associate Professor of Computer Systems Design at the University of Houston-Clear Lake. Dr. Bown also served as RICIS research coordinator.

Funding has been provided by the Engineering Directorate, NASA/JSC through Cooperative Agreement NCC 9-16 between NASA Johnson Space Center and the University of Houston-Clear Lake. The NASA technical monitor for this activity was William C. Young, of the Project Integration Office, Flight Data Systems Division, Engineering Directorate, NASA/JSC.

The views and conclusions contained in this report are those of the author and should not be interpreted as representative of the official policies, either express or implied, of NASA or the United States Government.

RICIS TECHNICAL NOTE

Integrity and Security in an Ada Runtime Environment

Principal Investigator

Rodney L. Bown

in partial fulfillment of

RICIS Task SE.26

June 1991

Integrity and Security in an Ada Runtime Environment

Rodney L. Bown
University of Houston-Clear Lake

RICIS task SE.26 proposed that the principal investigator (PI) participate in the 1990 Workshop on Issues of Integrity and Security in an Ada Runtime Environment. Funds and time were not available for the PI to participate. The proceedings from the workshop are published in [Ada90b]. A copy of the proceedings has been provided to the SE.26 task monitor.

This technical note provides a review of the Formal Methods group with additional commentary based on presentations and discussions with Dr. John McHugh [McHU90], [McHU91]. Dr McHugh was the leader of the Formal Methods working group.

Dr. Charles W. McKay of UHCL was the chair of the group that discussed the issues of Access Control in a Distributed Environment with Persistent Data. Dr. McKay has provided the Clear Lake technical community with comments related to this working group.

When one reads the Formal Methods section (section 3) of the proceedings, there is a temptation to dwell on the bitter tone of the group. An example is the statement "We are less than comfortable with the conceptual basis of the workshop". The group concentrated on process and not on a lengthy list of very specific issues. The group's contribution is that they have provided a list of research issues.

The group had difficulty in providing a formal definition of integrity. Dr. McHugh wrote:

> "Integrity is not a binary quantity but we seem to lack a metric for quantifying integrity. There is no basis for establishing the integrity of externally developed data or specifying the effects of software on the relationship between the integrity of input and output data. There is no basis for establishing the integrity metrics for software."

The integrity issue was discussed with Dr. McHugh during a February 1991 visit to the University of North Carolina. He emphasized that security can be represented with a discrete Boolean metric i.e. there has been a write down or a read up violation on a set of sensitive data.

He states that integrity is not a pure mathematical dual of security. As stated in the working group, the input data is part of the integrity domain. If the system observes a write up, is it an integrity violation? The new data itself may have higher integrity. An

weak analogy may be viewed within the context of equal data coming to Central Intelligence Agency: one set from an agent and another set from a CNN TV broadcast. The ability of the agent to write up to the CIA does not guarantee his data has a higher degree of integrity over the data provided by an on-the-scene CNN TV reporter.

The group provided a roadmap for research. One item of the roadmap and the final position statement are closely related to the space shuttle and space station. The group's position is to use a safe subset of Ada. Examples of safe sets include the Army Secure Operating System and the Penelope Ada verification tool. This PI recommends that a conservative attitude is required when writing Ada code for life and property critical systems. This requires the use of a safe subset of Ada. The benefit is that a developing tool such as Penelope may be sufficient to verify the safe subset.

The group complete their report with a position statement that is related to the developing Software engineering curriculum at UHCL and its support of RICIS research activities.

> "Incorporation of formal methods in software engineering practice requires a cooperative effort involving practitioners in the design and engineering of formal methodology and greater understanding and appreciation of software practice on the part of formal methods researchers.
>
> We therefore recommend a multi-threaded approach involving teams of researches and practitioners, preferably situated in the application development environment, to negotiate approximate solutions of real utility and strategies for extending them progressively more complete solutions."

Local activities related to this position statement include those cited below:

RICIS research activity with the Micro-electronics Computer Corporation (MCC) to evaluate Formal Methods.

UHCL is offering a Master of Science degree in Software Engineering Sciences. The bad news is that the degree should be called Software Engineering without the Sciences modifier. UHCL has proposed a name change for this degree.

This PI is offering a summer 1991 course in Formal Methods and Models. The good news is that there are 8 students in the class. The bad news is that 7 of the students are foreign.

The PI has submitted a RICIS research proposal to NASA JSC on using formal methods within the post delivery enhancement and configuration management activities of non-developmental (NDI) software.

The Ada 9X effort is directly related to this discussion. Dr. McHugh provided a report on Ada 9X at the November 1990 RICIS Conference [McHU91]. Dr. McHugh attended the Ada 9X Requirements Workshop held in Soderfors, Sweden on April 24-27., 1990. The Chair's report appeared in the September/October 1990 Ada Letters [Ada90a]. His notes have been provided to the task monitor. During this discussion Dr. McHugh expressed the view that in an attempt to be 100 percent upward compatible, Ada 9X will become too unwieldy for formal verification of the executable code. Locally Dr. Charles W. McKay has been coordinating the UHCL response to Ada 9X activities.

References

[AdA90a]
Boyd, Stowe. "Ada9X Requirements Workshop Soderfors, Sweden." Ada Letters. September/October 1990 104-128.

[Ada90b]
Proceedings from the 1990 Workshop on Issues of Integrity and Security in an Ada Environment. 3-5 April. Orlando, Florida. Sponsored by IIT Research Institute and Ada Joint Program Office. Published in Ada Letters November/December 1990 88-121.

[McHU90]
McHugh, John. Issues Related to Ada 9X. Presented at RICIS'90 Symposium. University of Houston-Clear Lake 7-8 November 1990.

[McHU91]
Private conversations with John McHugh, 8 February 1991.