Non-Developmental Item Computer Systems and the Malicious Software Threat

Rodney L. Bown

University of Houston-Clear Lake

April, 1991

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

NASA Johnson Space Center
Engineering Directorate
Flight Data Systems Division

ricis

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

TECHNICAL REPORT

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.

Non-Developmental Item Computer Systems and the Malicious Software Threat

Rodney L. Bown

University of Houston-Clear Lake

April, 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*

TECHNICAL REPORT

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

Non-Developmental Item Computer Systems and the Malicious Software Threat

Principal Investigator

Dr. Rodney L. Bown

Submitted in partial
fulfillment of

RICIS Task SE. 26

April 1991

TABLE OF CONTENTS

Non-Developmental Item Computer Systems and the Malicious Software Threat

1. Introduction

In 1985 the Department of Defense (DOD) published the Trusted Computer System Evaluation Criteria which is commonly called the "Orange Book" [DOD85]. This document establishes an evaluation criteria for judging the security properties of a computer system. Non-DOD computer users were quick to comment that the document does not provide any criteria to evaluate integrity or assurance of service properties. In spite of all its criticism, the Orange book has true value in that it provided an official set of security requirements for the design of secure systems.

Until recently, the Orange book indicates that the DOD has been willing to pay for the development of unique trusted computer systems to satisfy a high level of security. In addition, there have been several industrial efforts to design secure computer systems, Examples include but are not limited to an A1 level DEC VMS (not a commercial product), B2 level UNIX System V by AT&T, third party RACF and Top Secret software for IBM systems, and Secure ZENIX.

Reduced procurement budgets have now forced DOD and other government agencies to purchase non-developmental item (NDI) computer systems. These systems have not been design to satisfy any official set of security, integrity, and assurance of service (SI&A) requirements. This policy will increase the risk of using computer systems to support command and control functions. This is at time when the National Research Council has issue a report titled "Computers at Risk" [CLAR90]. The executive summary of this report states "Without more responsible design and use, systems disruptions will increase, with harmful consequences to society."

This paper reviews the context of NDI computer systems with respect to the malicious software threat and presents a set of post delivery criteria that an organization should establish in order to enhance the SI&A characteristics of NDI computer systems.

2. A DOD Developed System: The Army Secure Operating System

Computer systems have become critical components within DOD command and control systems. These systems require a high level of trust when used to command and control life and property resources. The requirement for trust usually exceeds the capabilities provided by most commercial computer systems. To meet this high level of trust, the DOD has procured unique computer systems in accordance with standards such as DOD-STD-2167/2167A [DOD88] and the Trusted Computer Assurance Criteria [DOD85]. This has required DOD to pay for the high development cost of these unique computer systems with no financial return of investment. The return on investment is restricted to the user's confidence that the system meets a unique set of high level military criteria for trust.

One such example is the development history of the Army Secure Operating System (ASOS). Three technical papers on ASOS were presented at the IEEE Computer Security and Privacy Conference in Oakland during May 1990 [WALD90], [DiVI90a], [DiVI90b]. As part of a software procurement, a DOD agency usually provides funds for the development of software tools that are associated with the procured system. Ownership of the tool development supports additional trust of the system. Reference [DiVI90b] describes the development of a knowledge based tool to support the formal verification of ASOS.

In early 1990, these papers indicated that ASOS is a technical success and that the system was being delivered to the U. S. Army for active use by appropriate units. Recent discussions have indicated that ASOS will not be deployed as originally intended due to its high cost and narrow application domain [HOFF90], [ARMY90]. These discussions have indicated the standard Army operating system will be a NDI POSIX compatible UNIX like system.

ASOS has provided another example of the procurement dilemma faced by government agencies such as NASA and DOD. These agencies have unique high level requirements that are not satisfied by commercial general purpose products. The 1980-90 computer system procurement decade has indicated that agencies such as DOD and NASA can not influence the general purpose computer market. These agencies must pay for the development of unique systems or they must modify their procurement criteria to match the availability of general purpose commercial systems. In order to reduce the risk of using NDI computer systems, these agencies must move their high level requirements from the procurement phase to the post delivery phase. During the post delivery phase the agency must support the design, development, or procurement of enhancements to the baseline delivered system.

3. Non-Developmental Commercial Computer Systems

Commercial computer vendors design general purpose systems that are meant to generate a wide based market response sufficient to recover their development costs through the delivery price of the system. Similar to government agencies, individual commercial customers can not influence the design of computer systems unless they are willing to pay for a major share of the development costs. The result is that each customer must purchase a NDI system from a trusted vendor, and then tailor the system to the unique requirements of the enterprise.

Commercial customers are primarily interested in two characteristics of computer systems: functionality and performance. Based on a risk analysis some customers have been willing to pay for assurance of service i.e. fault tolerant systems. In many systems, assurance of service is not part of the design criteria for the system. The Digital Equipment Corporation has sold more VAX systems without fault tolerance than has the Tandem corporation sold systems with fault tolerance. Tandem has made a market penetration into narrow application domains such as on-line banking and medical systems.

Customers of general purpose commercial systems, are not concerned about the heritage of the design and development tools used by the vendor. Many of these tools can be classified as Commercial Off The Shelf (COTS) tools that have a poor software engineering heritage. The customer is forced to rely upon the market place to provide consensus opinions about the trusted use of COTS software and hardware design tools used within the pre-delivery development phase of commercial systems. There is no authorized governmental or industrial agency that provides oversight and licensing of commercial computer systems.

There are significant counter examples within other technical disciplines that can impact the health and welfare of the general populace. Commercial aircraft must be designed and manufactured in accordance with stringent FAA standards. Automobiles must satisfy criteria established by the National Transportation Safety Board. Electrical appliances must satisfy criteria published by the Underwriters Industrial Laboratories (UIL).

4. Security, Integrity, and Assurance of Service (SI&A)

The majority of commercial customers have been unwilling to pay an up front premium delivery price for SI&A if it means that there will be decrease in functionality and performance. UNIX like systems have demonstrated adequate support for the general requirements of functionality and performance on modern general purpose computer systems. Commercial customers are willing to purchase UNIX based operating systems with known security and integrity discrepancies in order to obtain the functionality of the system.

If the customer identifies a need for SI&A, a set of individual and unrelated modifications and enhancements will be made to the system after its delivery. The installed system within each enterprise will then evolve along a unique modification path. Each enterprise will be required to maintain tight configuration management control over their unique computer system. When the vendor releases a new version of the baseline system, each enterprise will be required to revalidate the SI&A characteristics of the new system with the unique set of local SI&A components.

When NDI systems are procured for SI&A applications, there is a need to identify all COTS tools that were used in the design and development of the system. COTS tools are a potential source of malicious software. These tools should be purchased along with the system. The tools can then be examined to detect the presence of hidden malicious software. In addition the tools can be executed with a set of test software and data. The tools then become part of the total system configuration management plan.

5. Post Delivery SI&A and Malicious Software

In the last few years, the threat of malicious software has caused many commercial customers to be concerned about the SI&A of their installed computer systems. The SI&A of the system is usually provided by "after delivery procurement" of duplicate and/or backup systems, security policies and procedures, resetting of default parameters and passwords, and piece wise installation of security hardware and software components.

When the customer is unwilling to pay for the development of unique high performance systems that support SI&A, the customer is forced to move the SI&A criteria to the post delivery phase. The nature of the commercial post delivery phase is different from a typical DOD-STD-2167/2167A procurement phase.

The primary difference is related to the responsibility for configuration management through out the life cycle. If an organization or agency has paid for a computer system, it will have ownership of the system. Through out the life cycle, a configuration management contractor can maintain the consistency of all installed systems. New malicious software threats may negate the current SI&A protection mechanisms. The response to the new threat will require modification and/or enhancements to the system. The agency has the authority to authorize and monitor all prevention and detection enhancements and modifications to the system.

The operator of an NDI computer system does not have ownership of the development process. The life cycle configuration management of an NDI computer system is under dual and possibly conflicting control of a set of customers and the computer system vendor. The customers must respond to two parallel events that will cause a revalidation of the SI&A characteristic of the system.

The first event is the caused by the vendor's desire to modify the baseline system in response to the perceived needs of a general purpose market. The vendor will release new versions of the baseline system that may contain internal modifications that are incompatible with the customer's locally enhanced system. The customer will have to upgrade his baseline system and then revalidate the SI&A characteristics of the local system.

An example of this configuration management problem is related to device drivers and third party vendors of secure devices. A new version of the computer system may include changes to device drivers and to the vendor's own produced devices. If the customer is using devices developed by third party vendors, there may be incompatible interfaces between the device driver and the device. There may be an unacceptable time delay until the third party device vendor is able to release an upgrade kit.

The second event is caused by the need to respond to the threat of new malicious software. This will require modification to the SI&A mechanisms. The customer will be required to carefully manage the SI&A revalidation process with two independently moving targets: system versions and malicious software prevention mechanisms. The dilemma is that the customer must choose between three new configurations as summarized below:

baseline:	system version 0	with SI&A version 0
possible new configurations:		
configuration 1:	system version 0	with SI&A version 1
configuration 2:	system version 1	with SI&A version 0
configuration 3:	system version 1	with SI&A version 1

The maintenance of accurate documentation is closely related to the complexity of configuration management. The customer will be required to maintain the computer system documents, SI&A system documents, and a locally developed interface control document (ICD). When a new version of the baseline system is released, the customer will have to update the local ICD. Any updates to the SI&A components will require additional modifications to the ICD document. Each locally developed ICD will exhibit unique documentation standards and quality. This will decrease the portability of technical individuals between system sites.

An industrial supported user's group could provide the mechanism to establish consistent ICD's. The user's group would have to be established with a mandate to establish criteria to establish and monitor ICD's. This would required substantial finding support.

6. Computer System Unique Attributes

An NDI procurement policy has moved the implementation of unique computer system attributes from the design and development phase to the post delivery phase. During development, all unique attributes are controlled by software engineering paradigms supported by accurate documentation of the system requirements, specifications, and design. An example is the documentation requirements specified by DOD-STD-2167/2167A. This provides confidence that the delivered system will be a high fidelity implementation of the design documents. When a mismatch between design and implementation is observed, a discrepancy report (DR) or software change request (SCR) will be created. The set of DR's and SCR's form an addendum to the design documents that initiate a new iteration of the software life cycle.

The post delivery phase of an NDI system has a different set of constraints that were discussed in the previous section. Here the control mechanisms are limited to configuration management paradigms. The vendor's design and development documents may not be available to the customer. In some cases the vendor may classify the source code as proprietary. The customer may only receive the object code supported by a user's manual. In addition the vendor may claim that any customer modifications made to the delivered system will negate the warranty.

These issues may require the customer to purchase source code and design documentation within very tight nondisclosure agreements. These post delivery issues will increase the cost of a NDI system. It is pure speculation to estimate the value of the cost increase factor. It is sufficient to state that NDI procurement contains additional post delivery costs that must be considered for each case.

7. Positive Feedback to Commercial Computer System Vendors

In the long term, a NDI computer system procurement policy may promote an improvement in the commercial market for SI&A. As the trust of each NDI computer system is enhanced by individual customers, the original vendor may be motivated to include the enhancements in future versions of the baseline system. The vendor holds the rationale and knowledge of the system design. The vendor should be able to incorporate SI&A enhancements within a system context using all proper software engineering paradigms and procedures. All organizations should encourage all NDI vendors to critique third party SI&A mechanisms for potential incorporation into future versions of the baseline system.

8. NDI Computers and Software Safety

Software safety has become an additional issue within the context of trusted computer systems. Susan Gerhart of MCC, Austin, Texas provided a review of Formal Methods for Trustworthy Systems at the RICIS'90 Symposium [GERH90]. The point to be observed within the context of this paper is that formal methods have not been used to design and develop known NDI computer systems. It is conceivable that a limited use of formal methods could be applied during a post delivery re-engineering effort of discrete SI&A components.

Another issue is the academic training and licensing efforts related to life and property computer systems. There are substantial efforts in the United Kingdom and European communities to enforce a licensing paradigm for software practitioners that are developing life and property critical systems. If an organization plans to use an NDI computer system to control life and property, the licensing paradigm must be addressed during the post delivery re-engineering effort.

9. Summary and Recommendations

In summary it must be understood the a NDI procurement policy will increase the risk of using computer systems to support life and property critical functions. This risk can be reduced by establishing a set of post delivery trusted computer criteria.

This paper has discussed the issues and rationale related to developing a set of NDI post delivery criteria for life and property critical computer systems. A proposed set of criteria is listed on the next three pages.

CRITERIA

NDI Post Delivery Criteria to Enhance the Security, Integrity and Assurance of Service for Command and Control Computer Systems

NDI:	Non Developmental Item
SI&A:	Security, Integrity, and Assurance of Service
ICD:	Interface Control Document
COTS:	Commercial Off The Shelf

1. A quantitative SI&A risk analysis shall be applied to each NDI procurement of command and control computer systems.

   Rationale: There is a need to determine the risk of using a NDI computer system to support a command and control computer system. The result of the quantitative risk analysis will provide guidance to estimate the budget required to support specified post delivery SI&A activities.

2. A post delivery SI&A configuration management plan shall be developed for each NDI computer system.

   Rationale: This plan is needed to determine the resources necessary to provide post delivery SI&A support for the NDI system.

3. A post delivery SI&A budget shall be developed to support post delivery activities.

   Rationale: This plan is needed to determine the estimated cost of post delivery SI&A activities. The cost estimate should consider the cost of materials, personnel, and training.

4. A separate NDI computer system shall be procured to establish a configuration management facility to support the design/procurement and testing of all post delivery modifications to the installed systems.

   Rationale: NDI procurement policy must provide for the establishment of a facility to support verification and validation (V&V) activities related to post delivery modifications.

5. For each post delivery modification to the NDI system, an ICD shall be created and maintained by the organization responsible for the configuration control facility cited in 4 above.

   Rationale: The V&V facility will be used to support in house activities to enhance the SI&A of the NDI system and the validation of the ICD.

6. All COTS tools used to develop the NDI system shall be procured and maintained by the organization responsible for the configuration control system cited in 4 above.

   Rationale: COTS tools are a potential source of malicious software. This is necessary to verify the trust of all COTS design tools.

7. NDI computer systems shall be procured with warranties that permit controlled modification by the procuring agency.

   Rationale: It is assumed that SI&A enhancements will be necessary during the post delivery phase of the computer systems. These enhancements should not negate normal warranty conditions of the baseline system.

8A. The NDI computer shall be delivered with detailed documentation that is sufficient to provide guidance to non-vendor post delivery SI&A design, and test activities.

   Rationale: It is assumed that in agency organizations or third party vendors will be the source of mechanisms that will be installed to enhance the SI&A of the computer system. Detailed documentation is required to support the design and test activities of these non-vendor organizations. When the vendor releases a new version of the baseline system, the agency will be required to revalidate the trust of all non-vendor mechanisms. Detailed documentation is required to support the revalidation activity.

8B. (Alternative or in partial addition to 8A) The NDI vendor shall designate and provide access to a stand alone duplicate computer system in order to validate in agency and/or third party SI&A mechanisms.

   Rationale: The NDI vendor may withhold some detailed design documentation based on competitive considerations for proprietary information. The vendor has the right to protect proprietary data. A vendor controlled computer system should then be provided to support test and validation activities for non-vendor SI&A mechanisms.

9. Post Delivery Re-Engineering Effort

The customer shall provide a re-engineering effort to apply formal methods to SI&A components. This effort must be accomplished by licensed practitioners. This should be done with the support from the NDI vendor or a user's group.

Rationale: This effort will provide a baseline for an investment in efforts related to application of formal methods by licensed practitioners.

REFERENCES

[ARMY90]
Discussions at U. S. Army HQ CECOM 16 August 1990.

[CLAR90]
Clark, David, editor. Computers at Risk. Washington: National Academy Press, 1990.

[DiVI90a]
Di Vitto, Ben L., et. al. "Specification and Verification of the ASOS Kernel." Proceedings of the IEEE Computer Society Symposium on Research in Security and Privacy. 7-9 May 1990. Oakland, California. pp. 61-74.

[DiVI90b]
Di Vitto, Ben, et. al. "The Deductive Theory Manager A Knowledge Based System for Formal Verification." Proceedings of the IEEE Computer Society Symposium on Research in Security and Privacy. 7-9 May 1990. Oakland, California. pp. 306-318.

[DOD85]
United States Department of Defense. Command, Control, Communications and Intelligence. Department of Defense Standard. Department Of Defense Trusted Computer System Evaluation Criteria. DOD 5200.28-STD. December 1985. "The Orange Book."

[DOD88]
DOD-STD-2167 4 June 1985 and DOD-STD-2167A 29 February 1988.

[GERH90]
Gerhart, Susan. "An Assessment of Formal Methods for Trustworthy Systems." Proceeding of the RICIS Symposium. 7-8 November 1990. Houston, Texas.

[HOFF90]
Discussions with Hoffman and Associates, 25-27 June 1990.

[WALD90]
Waldhart, Neil A. "The Army Secure Operating System." Proceedings of the IEEE Computer Society Symposium on Research in Security and Privacy. 7-9 May 1990. Oakland, California. pp. 50-60.