A DOCTORAL PROGRAM WITH SPECIALIZATION IN INFORMATION SECURITY

A High Assurance Constructive Security Approach

Cynthia E. Irvine and Timothy E. Levin
Department of Computer Science, Naval Postgraduate School, Monterey, California

Abstract: A doctoral program in computer science with a specialization in information security is described. The focus of the program is constructive security. Key elements of the program are the strong computer science core upon which it builds, coursework on the theory and principles of information assurance, and a unifying research project. The doctoral candidate is a member of the project team, whose research contributes to the goals of the project and to fundamental advancements in high assurance security.

Key words: Information assurance, education, doctoral program

1. INTRODUCTION

As computing platforms become smaller, increasingly pervasive, and highly networked, the rampant exploitation of system vulnerabilities represents a threat to our ability to safely use information technology. Those who choose to wreak havoc on our systems do so with impunity. Fear that flawed systems may invite problems ranging from the annoyances of spam, identity theft, and loss of productivity, to catastrophic damage to critical information is turning computing from an enabling to a disabling technology. We are faced with the prospect that Gresham's Law will once again hold: the bad will drive out the good.

To address these problems in a military context, the Center for Information Systems Security Studies and Research (CISR) at the Naval Postgraduate School (NPS) has developed a program in Information

Assurance and Security education that addresses a broad range of information security issues through education and research. An important element of that program is the nurture of doctoral students.

1.1 Computer Science Ph.D. Program Overview

To conduct doctoral research in information security at NPS, one must look to the Computer Science Department. NPS started its Computer Science program in the mid 1970s and has offered Ph.D. degrees, i.e. research doctorates, for over two decades. The majority of students at the Naval Postgraduate School are engaged in a terminal Master's Degree program, while a smaller number are involved in the doctoral program. The Ph.D. program meets several objectives by providing educators to military universities, research-level personnel to oversee a wide range of technical projects in the military and government, and researchers in government laboratories.

The duration of the Computer Science Ph.D. program is three years for full time students. This may seem short relative to the four to five years usually required for doctoral students at other U.S. institutions, however NPS students are atypical with respect to the benefits afforded them. First, their tuition is paid for in its entirety by a sponsoring entity such as one of the military services or the U.S. Government. Second, each student continues to receive a pre-student salary from the sponsoring organization. Thus, the students have the freedom to pursue their studies without the distraction caused by attempting to offset their educational costs through external employment. Their work is also accelerated because NPS is on a year-round calendar with four full quarters of teaching and research per year.

In general, applicants to the Ph.D. program in Computer Science at NPS must have a Master's Degree in Computer Science or closely related field. Admission to NPS requires the submission of certified transcripts of all courses taken at the university level, both undergraduate and graduate. Graduate Record Examination scores are required for applicants not currently at NPS. It is expected that all grades and scores will be above average. Supporting material, such as Masters thesis, research reports, or published papers, that demonstrates the candidate's ability to conduct research is also encouraged. International students and non-native English speakers are required to score well on the TOEFL examination as a requirement for admission to the NPS Ph.D. program.

A Master's degree in Computer Science is an expected prerequisite. In some fields, the Master's degree is considered a "consolation prize" for students failing to pass certain examinations for the doctoral degree. This means that these programs often admit students with the intent of taking

them directly to the doctorate without stopping for a Master's degree. In contrast, a Master's degree in Computer Science is deemed a valuable terminal degree and is a generally expected milestone.

The funding model for Ph.D. programs at NPS is quite different from that of most other U.S. universities. Military and government civilian students are sponsored by a military service or agency. Thus, all of tuition and salary (at the pre-student income level) is paid for by external sources and does not have to be sought by the faculty Ph.D. supervisor. Some doctoral students are existing employees who have been involved in ongoing research projects. In such cases, the dissertation advisor is obliged to seek continued research support for the dissertation research through scholarships or research grants from a variety of funding agencies such as the National Science Foundation, the Office of Naval Research, the Defense Advanced Projects Research Agency, etc.

Support is also possible through industry as several of our ongoing research projects in cyber security involve industry partners. Usually these partnerships revolve around the use of specialized equipment or software, but they occasionally include financial support. We discourage doctoral students from engaging in proprietary or classified research, since the results would have restricted distribution and therefore not be considered a contribution to the overall body of knowledge in Computer Science, a requirement for a successful dissertation.

Each doctoral candidate is required to demonstrate knowledge of core computer science by passing a written qualifying examination. In addition, students must meet requirements in a minor subject and must pass an oral qualifying examination, the latter before commencing dissertation research. Upon completion of the dissertation, the candidate must defend the work in an oral examination.

1.2 Information Assurance and Security Specialization

Over the past decade, the thirteen quarter-long information security courses listed in Table 1 have been developed and are offered by the Computer Science Department. Many prerequisites are cumulative, i.e. Operating Systems requires Discrete Mathematics, Data Structures, Computer Architecture, and an appreciation of programming fundamentals.

Table 1. Information Assurance and Security Courses with their Prerequisites

Course	Course Title	Prerequisites	Students	
			MS	Ph.D.
CS3600	Introduction to Information Assurance	Computer Architecture	✓	✓
CS3640	Analysis of DoD Critical Infrastructure Protection	CS3600	✓	✗

Course	Course Title	Prerequisites	Students	
			MS	Ph.D.
CS3670	Secure Management of Systems	CS3600	✓	✗
CS3675	Network Vulnerability Assessment	CS3600	✓	✗
CS3690	Network Security	CS3600, Networking	✓	✗
CS4600	Secure Systems	CS3600, Networking, Operating Systems	✓	✓
CS4603	Database Security	CS3600, Databases, Operating Systems	✓	✗
CS4605	Security Policies, Models and Formal Methods	Discrete Mathematics, CS3600, Algorithms	✓	✓
CS4610	Information Ethics	none	✓	✗
CS4614	Advanced Topics in Computer Security	CS3600, CS4600, CS4605	✓	✓
CS4677	Computer Forensics	CS3600, CS3670, Computer Architecture	✓	✗
CS4680	Introduction to Certification and Accreditation	CS3600, CS3670, CS3690	✓	✗
CS4685	System Certification Case Studies	CS3600, CS3670, CS4680	✓	✗

Masters students may enroll in all of the courses listed in Table 1, while doctoral students enroll in selected (checked) courses intended to prepare them for dissertation research. Candidates in the Information Assurance and Security specialization generally meet their minor requirements by enrolling in courses in Mathematics or Electrical and Computer Engineering. A more concrete binding to the minor is achieved by having the non-Computer Science Dissertation Committee member come from one of those departments.

Dissertation research consumes the vast majority of a doctoral candidate's time. While prior experience and learning may shorten the duration of a candidate's research program, there is currently no formal recognition of those achievements. For example, a candidate with significant experience in the use of formal methods for high assurance development would have a head start when embarking on a program of related research.

Research for a Ph.D. requires that each student conduct dissertation research on an original topic that results in a new contribution to the field of computer science and, in this case, information security. The size of the dissertation is of less importance than its quality and contribution. (Louis de Broglie (1923) provides an example of high quality brevity.)

2. UNIFYING HIGH ASSURANCE RESEARCH PROJECT

Doctoral research is generally centered around a unifying research project being conducted by a member of the faculty. Currently CISR has embarked on the *Trusted Computing Exemplar* (TCX) Project (Irvine et al. 2004b), which provides a context for Masters theses and Ph.D. dissertation research. A brief motivation for and description of this effort follows.

2.1 Motivation

Much of the global critical infrastructure has now been constructed using commodity systems and depends upon "layered defenses" for which there is no well-founded protection model (Schell 2001). Through a process of constructive security engineering it is possible to describe security architectures for which there is a concrete protection model (Irvine 2003). These architectures can combine both commodity elements and components at selected junctures that provide high assurance of correct policy enforcement as well as evidence that they have not been subverted (Irvine 2004a). The TCX project is motivated by a recognition that construction of high assurance systems has not been a priority in the commercial sector. Even during the 1970s and 1980s, only a few score people contributed to the construction of high assurance systems and information was insufficiently detailed at best (Gasser 1988, Schell et al. 1973). To exacerbate the esoteric nature of these systems, those that were successfully developed were classified or proprietary. Market-driven academic institutions have not invested in course materials that teach the concepts of high assurance secure systems development in a coherent manner. Thus, we lack the availability of high assurance trusted systems, developers who can create these systems, as well as public domain worked examples upon which new projects could be modeled.

2.2 Trusted Computing Exemplar Project

The *Trusted Computing Exemplar Project* is intended to provide an openly distributed ***worked example*** of how high assurance trusted computing components can be built. It encompasses four related activities: creation of a prototype framework for rapid high assurance system development, development of a reference-implementation trusted computing component, evaluation of the component for high assurance, and open dissemination of results related to the first three activities. Each of these is discussed in greater detail below.

2.2.1 Rapid high assurance system development framework

A prototype *high assurance development framework* is being created, and used to design and develop a reference implementation *trusted computing component,* the *TCX Separation Kernel.* High assurance methodologies and techniques are applied during the entire lifecycle. The TCX project is using openly available tools for the development framework; these tools are selected on the basis that they do not impose restrictive licensing requirements upon the results of the effort. The prototype framework for rapid high assurance development is intended to provide a set of interoperable tools and define a set of efficient, repeatable procedures for constructing trusted computing systems and components.

2.2.2 Reference-implementation trusted computing component

We are developing a high assurance, embedded micro-kernel, and trusted application, as a reference implementation exemplar for trusted computing. The TCX Separation Kernel will enforce process and data-domain separation, while providing primitive operating system services sufficient to support simple applications.

2.2.3 High assurance Evaluation

Under sponsorship from the National Security Agency, we are the lead writers of a Separation Kernel Protection Profile. This effort will result in an official NSA protection profile, which will be used for the evaluation not only of our Exemplar Separation Kernel, but also of a wide range of trusted separation kernels. This work is a key first step toward evaluation.

2.2.4 Open dissemination of results

To provide materials to other educators who want to learn about and teach the techniques of high assurance design, development and engineering, we will make all of the results of our activities available. The documentation, source code, development framework and other evidence for a third-party evaluation will be made *openly available* as they are produced, providing previously unavailable examples of "how-to" for high assurance trusted computing. This will include not only the code and evaluation documentation, but descriptions of the analysis and decisions that took place in our efforts.

A wide range of research topics has emerged from the TCX activities. Examples include surveys and applications of formal methods; modeling; hardware analysis; protocol analysis; development of materials related to Common Criteria evaluations; and tools design and implementation. The TCX project has already provided thesis areas for two graduated Masters students and, currently, the effort provides research topics for six Masters students and two doctoral candidates. The breadth and depth of the project will continue to accommodate future students.

An advantage of the overarching project is the involvement of the student as part of a larger team tackling a wide range of project-related research and development. In choosing a model for a unifying research project, Multics (Corbato 1965) was viewed as a highly successful example. Even though the student may concentrate his or her thesis or dissertation research on a small, highly focused research topic, the exposure to the work of others and the appreciation of the challenges associated with high assurance secure technology contributes to a broader perspective. Often, the research projects benefit from the insights drawn from the operational experiences of the students.

3. CONCLUSION

A research doctoral program has been described. It is based upon a core in computer science and provides both classes and research in computer and network security. A theme underlying all coursework and research is that of improving cyber security through constructive security engineering. Through a unifying research project doctoral research is given a context. The team approach provides a stimulating learning environment.

REFERENCES

de Broglie, M. L., 1923, Ondes et quanta, *Comptes rendus,* Vol. 177, pp. 507-510.

Corbato, F.J. and Vyssotsky, V.A. 1965. Introduction and Overview of the Multics System, *Proceedings of AFIPS Federal Joint Computer Conference,* pp. 619-628.

Irvine, C.E., 2003, Teaching Constructive Security. *IEEE Security and Privacy,* 1(6):59–61, November.

Irvine, C.E., Levin, T.E., Nguyen, T.D., Shifflett, D., Khosalim, J., Clark, P. C., Wong, A., Afinidad, F., Bibighaus, D. and Sears, J., 2004a, Overview of a High Assurance Architecture for Distributed Multilevel Security. To appear in *Proceedings of of the 5th IEEE Information Assurance Workshop,* West Point, NY, June.

Irvine, C.E., Levin, T.E., Nguyen, T.D., and Dinolt, G.W., 2004b, The Trusted Computing Exemplar Project, To appear in *Proceedings of the 5th IEEE Information Assurance Workshop,* West Point, NY, June.

M. Gasser, M, 1988, *Building a Secure Computer System,* Van Nostrand Reinhold, NY, NY.

Schell, R. R. 2001. Information Security: Science, Pseduoscience. *Proceedings of the 17th Annual Computer Security Applications Conference,* pp. 205–216, New Orleans, LA, December.

Schell, R.R., Downey, P.J., and G. J. Popek, G.J., 1973,, Preliminary Notes on the Design of Secure Military Computer Systems. Technical Report MCI-73-1, Electronic Systems Division, Air Force Systems Command, Hanscom AFB, Bedford, MA, 73.