Security Informatics: A Paradigm Shift in Information Technology Education

Susan M. Merritt
Allen Stix
Judith E. Sullivan
The present paper was accepted as an extended abstract for a poster at ISI 2004, the 2nd Symposium on Intelligence and Security Informatics.

ISI 2004 was held on June 10 - 11, 2004, at the University of Arizona in Tucson, Arizona.

Pages 9-10 herein is the poster that appears in the published proceedings.

Susan M. Merritt is the Dean of the School of Computer Science and Information Systems at Pace University and Professor of Computer Science.

Allen Stix is Associate Professor of Computer Science at Pace University, based in Westchester.

Judith E. Sullivan holds a Master of Science in Computer Science from Pace University and is the Assessment/Research Analyst for the School of Computer Science and Information Systems at Pace University.
Security Informatics:
A Paradigm Shift in Information Technology Education

A short paper by
Susan M. Merritt, Allen Stix, and Judith E. Sullivan
School of Computer Science and Information Systems
Pace University, New York, NY

Abstract

Security informatics will represent a paradigmatic shift in college and university curricula in computer science, software engineering, information systems and science, networking and telecommunications, Internet technologies and related disciplines – the disciplines that might be assumed under the broad umbrella of “information technology” – though most programs have not yet understood the import or implemented the systemic change. Faculty have experienced much technology change over the short history of computing and are much more frequently introducing change into courses and programs than their colleagues in other disciplines. Nevertheless, most change to date is local to courses and programs. The systemic change needed to appropriately incorporate security into these curricula is compared to that which occurred around object technology, both in response to systemic change in the computing industry. A conceptual model is cited. Moreover, the need for security in information applications in virtually every discipline will generate robust interdisciplinary and multidisciplinary opportunities for informatics (as different from information technology) programs.
Introduction

College and University faculty in computer science, software engineering, information systems and science, networking and telecommunications, Internet technologies and related disciplines—the disciplines that might be assumed under the broad "umbrella" of information technology—routinely confront new technologies and incorporate those into educational programs for undergraduates and graduate students. The adaptation is generally "local" to a course (e.g. adding a module), to a set of electives (e.g. creating a new elective), or to a program (e.g. changing a platform or a programming language). Examples abound. Just one example might be the introduction of a project course surrounding hand-held devices (e.g. the J2ME and its use with personal digital assistants, telephones and other "pervasive" devices).

Every now and then, however, there are paradigm shifts. The new technology is of such scope and significance that it calls for systemic change. The conceptual models for the structure of systems, programs, data, or problem-solving change. Instead of representing local adjustments to educational programs, the technology affects the content and presentation of nearly every course in a curriculum. Again, examples abound over the short history of computing including a move from mainframe processing and timesharing to microcomputers and distributed computing; to client-server systems; to a new magnitude of networking with the Internet; and most recently to the "object paradigm" in software development.
Comparing two curricular paradigm shifts

Over the last 10 years or so education in computing has been transformed by the object paradigm. Once object orientation moved from the research and development laboratories, industry embraced it as a critical approach to building increasingly complicated systems with improved effectiveness and efficiency. Similarly with society's increasing dependence upon automated information systems – and in the face of enhanced risk to these systems – research and development programs in security have accelerated and both industry and the public sector have begun to demand security technologies to provide the required reliability.

Just as objects profoundly affected the content of courses in programming, analysis and design, project management, and software engineering; so will security. The academic content of security ranges from technical issues on the programming level (e.g. understanding and implementing code signatures and certificate management) to the creation of software features and tools making it possible for organizations to customize security policies and procedures. Security areas range from the server-side to the client-side (e.g. installing a firewall and virus protection, learning about browser-supplied facilities, and policies relating to information back-up). They range from issues of electromagnetic propagation during computing to planning for recovery from physical disaster.

When objects were new to practitioners they were already being used by researchers and developers from whom expertise became available
to industry. And so it is with security. Pieces on security are appearing in popular computing magazines (e.g. PC Magazine; October 1, 2003; "Total Security" by Cade Metz) and with greater frequency in professional journals. In fact, the IEEE has just launched a new security journal, the IEEE Transactions on Dependable and Secure Computing. Publishers are rapidly bringing out new books and booksellers are increasing shelf space for the computer security section. Security has moved from research and development laboratories to the industry at large.

In the early days of objects – and in some programs still – there was a good deal of local curricula change in colleges and universities without an understanding of the pervasive effect of this fundamental new technology. Leaders grasped the paradigm and made systemic change. Such is the case with security.

Security across the curriculum

The National Security Agency (NSA) with its curricula certification and center of excellence designations is encouraging colleges and universities to assess where security surfaces within their course offerings and provides a guide to how and where coverage may be strengthened or augmented.

Even more important, the NSA offers a typology, created by John R. McCumber, for curriculum evaluation and planning. It is a conceptual model that is practical, comprehensive, and transcends particular
technologies and products. This typology has the potential, if used creatively and effectively, to enable the organization of security content with elegance and pervasiveness, and thereby to approach and ultimately achieve systemic change in college curricula.


Pfleeger identifies security with respect to maintaining the confidentiality, integrity, and availability of the system's information:

- **confidentiality** - information is viewable only by authorized parties (this is often characterized as privacy)

- **integrity** - information is modifiable only by authorized parties and only in prescribed ways (information should not become corrupted)

- **availability** - information is available to authorized parties when expected (the system should not be down when it is supposed to be in service)
These are the three concerns related to information security and therefore the categories of activity pertinent to securing automated information systems.

System vulnerabilities (i.e. potential weak points), the various kinds of threat, and the prospective methods of defense can be studied with greater precision by examining each concern together with the locus of information: in transmission, in storage, in processing, creating the two dimensional model depicted below:

```
transmission  storage  processing
```

<table>
<thead>
<tr>
<th>confidentiality</th>
<th>X</th>
<th>X</th>
<th>X</th>
</tr>
</thead>
<tbody>
<tr>
<td>integrity</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>availability</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

Finally, as overlays on this matrix, McCumber specifies a technology layer, a policy and practice layer, and an education, training, and awareness layer. These identify the perspective from which vulnerabilities, threats, and defenses are considered. The technology layer, focused on hardware and software, might include the strengths and weaknesses of encryption algorithms used for information transmission, or use of the Java verifier to check downloaded applets in .class files for array bounds violations that would compromise the
confidentiality of information in processing. The layer associated with policy and practice pertains to establishing the procedures to be followed in working with information systems (e.g. acceptable passwords, the storage of CDs). The layer of education, training, and awareness includes sensitizing software developers, engineers, and users to the principles of information security and the protection of information. Lest user education seem peripheral, consider the piece on the 2/5/04 front page of the New York Times titled “Geeks Put the Unsavvy on Alert: Learn or Log Off” that was prompted by the MyDoom virus. The article concludes with a “reminder to users” from Scott Charney, Microsoft’s chief security strategist. He states that users “have a responsibility to be careful and protect themselves.”

This model provides a very useful conceptual typology that enables the elements of this new technology of security to be organized throughout a curriculum or set of curricula. At the same time it is sufficiently flexible to enable a creative paradigmatic approach to systemic change in the curricula.

Security Informatics

Among at least some information technology educators in the United States (e.g. the “IT Deans” group sponsored by the Computing Research Association --the CRA) there is a growing understanding of “informatics” as information technology in an interdisciplinary or multidisciplinary context (thereby with more breadth than the traditional European understanding of “informatics” as synonymous with computer science).
Because of the extraordinary need for information security in virtually all contexts, the systemic inclusion of security technologies in information technology programs make them more attractive than ever for cohort programs in many other disciplines. This is an approach undertaken at our institution as we develop information security programs with criminal justice and biology, and introduce security into our collaborative information technology programs in health care, public administration, business, and education.
Security Informatics:
A Paradigm Shift in Information Technology Education

Susan M. Merritt, Allen Stix and Judith E. Sullivan
School of Computer Science and Information Systems
Pace University, New York, NY

The requirements for security in all information applications is generating interdisciplinary and multidisciplinary needs for security informatics programs. Security informatics is propelling a paradigm shift in college and university curricula as awarenesses, practices, products, and theory are added to address the sweeping demands of information assurance.

Confidentiality, integrity and availability are the three principles of computer security:

<table>
<thead>
<tr>
<th>confidentiality</th>
<th>information is viewable only by authorized parties (this is often characterized as privacy);</th>
</tr>
</thead>
<tbody>
<tr>
<td>integrity</td>
<td>information is modifiable only by authorized parties and only in prescribed ways (information should not become corrupted);</td>
</tr>
<tr>
<td>availability</td>
<td>information is available to authorized parties when expected (the system should not be down when it is supposed to be in service).</td>
</tr>
</tbody>
</table>

System vulnerabilities (i.e. potential weak points), the various kinds of threats, and the prospective methods of defense can be studied with greater precision by examining each principle together with the locus of information: in transmission, in storage, in processing. The cells in the resulting two-dimensional model may be approached on three levels. The levels relate to technology (T), practices including policy formulation (P), and awarenesses including education and training (A).
<table>
<thead>
<tr>
<th>confidentiality</th>
<th>storage</th>
<th>processing</th>
</tr>
</thead>
<tbody>
<tr>
<td>T/P/A</td>
<td>T/P/A</td>
<td>T/P/A</td>
</tr>
</tbody>
</table>

Questions

Can the scope of practices and technologies associated with information assurance be accommodated by current curricula or will curricula be fundamentally changed?

How can the transient technology of digital security be dissociated from the transcending, enduring concepts?

How does security informatics presage a change of paradigmatic magnitude in technology education?

References


The School of Computer Science and Information Systems, through the Technical Report Series, provides members of the community an opportunity to disseminate the results of their research by publishing monographs, working papers, and tutorials. *Technical Reports* is a place where scholarly striving is respected.

All preprints and recent reprints are requested and accepted. New manuscripts are read by two members of the editorial board; the editor decides upon publication. Authors, please note that production is Xerographic from the pages you have submitted. Statements of policy and mission may be found in issues #29 (April 1990) and #34 (September 1990).

Please direct submissions as well as requests for single copies to:

Allen Stix  
School of CS & IS - Suite 412 Graduate Center  
Pace University  
1 Martine Avenue  
White Plains, NY 10606-1932