Towards Standards in Digital Forensics Education

Peter Cooper
Sam Houston State University
Department of Computer Science
College of Arts and Science
Huntsville TX 77341 USA
1.936.294.1569
cooper@shsu.edu

Gail T. Finley
University of the District of Columbia
Department of Computer Science
and Information Technology
Washington, DC 20008 USA
1.202.274.6271
gfinley@udc.edu

Petteri Kaskenpalo
AUT University
School of Computing and
Mathematical Sciences
Auckland, New Zealand
64.9.9219999
petteri.kaskenpalo@aut.ac.nz

Agenda

- Purpose
- Concern
- Approach
- Professional Spaces
- Knowledge Areas
- Digital Forensics Domain
- Challenges
- Conclusions

Purpose

- *…to begin the process of delineating the problem space uniquely occupied by Digital Forensics and thus clarifying the distinction between Digital Forensics and other computing disciplines.*

- *…through an evaluation of the knowledge areas represented in existing Digital Forensics academic offerings and an assessment of the relative importance of those knowledge areas.*

Concerns

- *As a result of both social, industrial and government pressures, a significant professional need has emerged to provide "…scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations".* [Digital Forensics Certification Board]

Concerns

- *While the demand for continuing professional education and certification has led to the initial development of lower level programs, courses, and training modules it does not address the need to develop a coherent academic cadre to provide the research and academic sustainability necessary to further the discipline. The growth in advanced courses similarly is designed to meet professional needs.*

Professional spaces

- A durable domain of human concern
- A codified body of principles (conceptual knowledge)
- A codified body of practice (embedded knowledge),
- Standards for performance
- Standards for ethics and responsibility.

(Denning 2001, *Communications of the ACM*)

Professional spaces

- Law enforcement
- Legal
- Judicial
- Business & Industry
- Science & technology
- Education
- Government

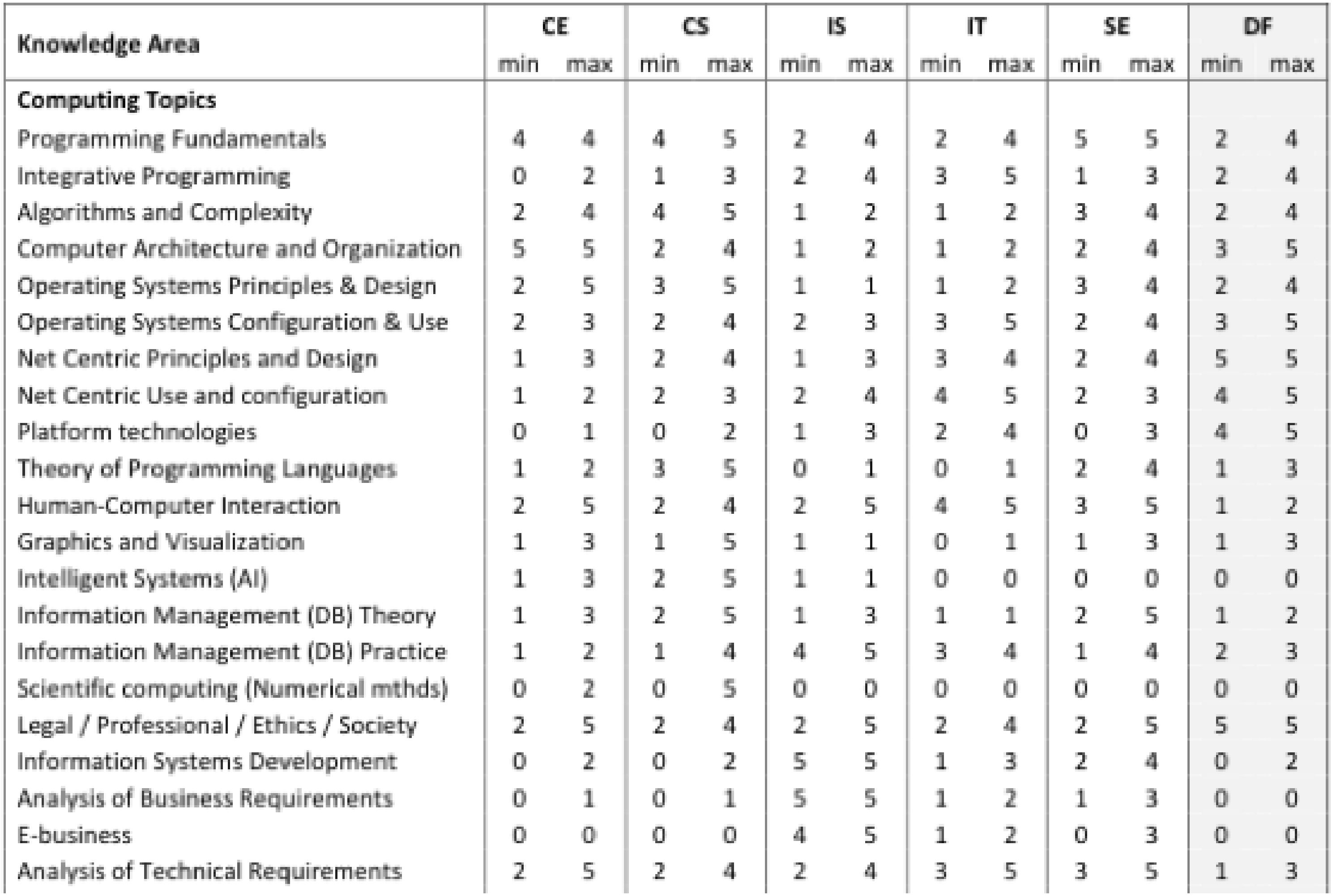
Professional spaces

- First Responder
- Digital Forensics Investigator
- Digital Forensic Analyst
- Digital Forensics Researcher
- Digital Forensics Educator

Knowledge Areas

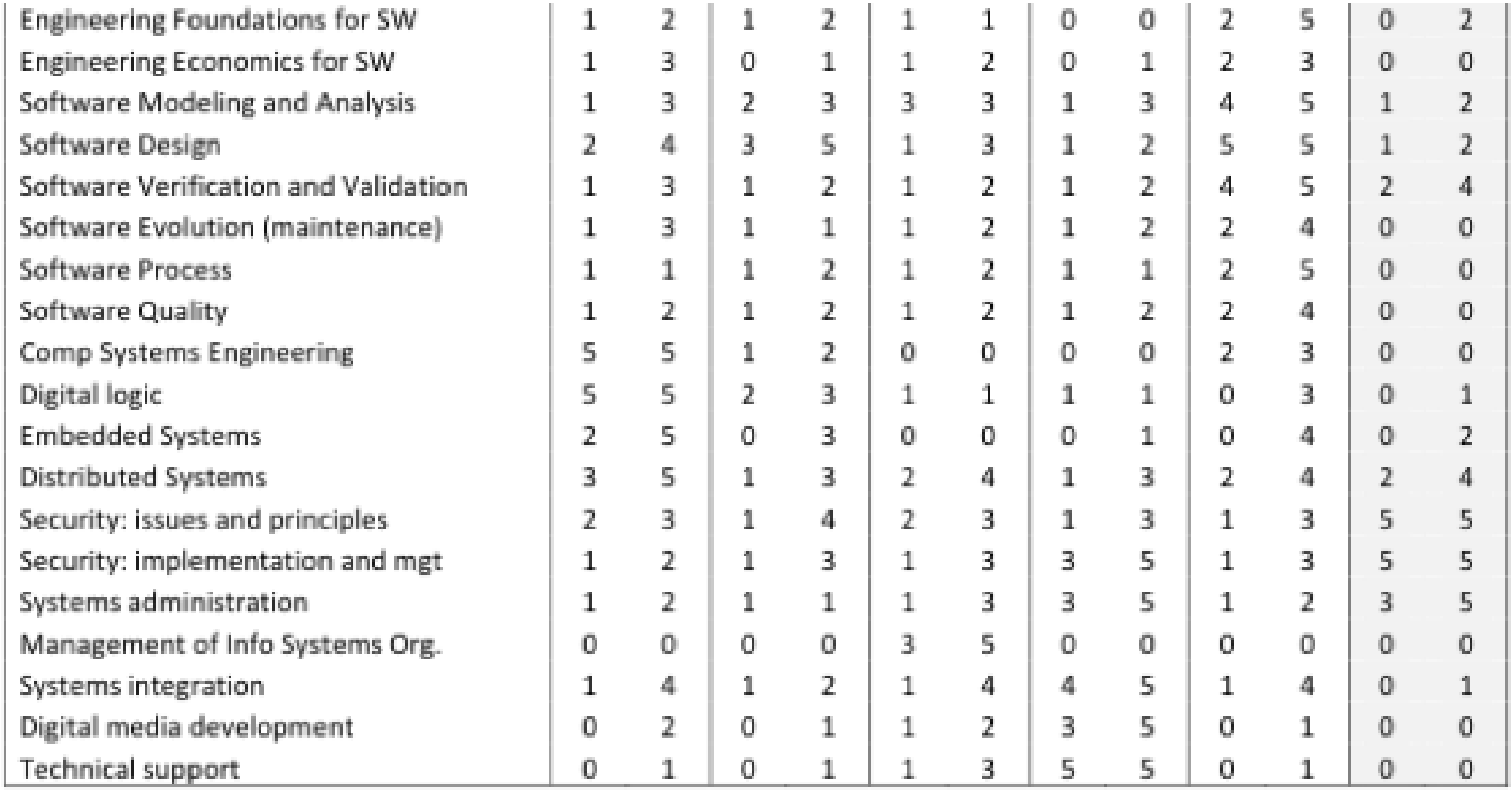
- Crime scene investigation
- Forensic analysis
- Law
- Ethics
- Computer science
- Electronics
- Mathematics

Knowledge Areas



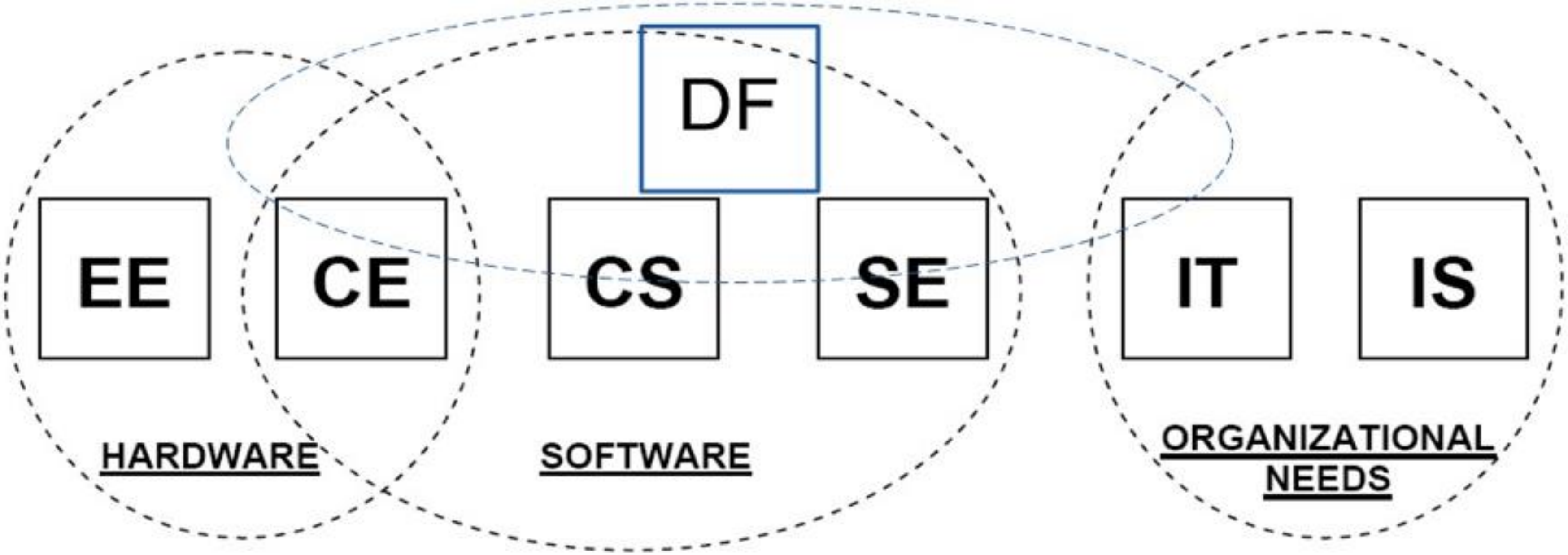
Knowledge Area	CE		CS		IS		IT		SE		DF	
	min	max	min	max	min	max	min	max	min	max	min	max
Computing Topics												
Programming Fundamentals	4	4	4	5	2	4	2	4	5	5	2	4
Integrative Programming	0	2	1	3	2	4	3	5	1	3	2	4
Algorithms and Complexity	2	4	4	5	1	2	1	2	3	4	2	4
Computer Architecture and Organization	5	5	2	4	1	2	1	2	2	4	3	5
Operating Systems Principles & Design	2	5	3	5	1	1	1	2	3	4	2	4
Operating Systems Configuration & Use	2	3	2	4	2	3	3	5	2	4	3	5
Net Centric Principles and Design	1	3	2	4	1	3	3	4	2	4	5	5
Net Centric Use and configuration	1	2	2	3	2	4	4	5	2	3	4	5
Platform technologies	0	1	0	2	1	3	2	4	0	3	4	5
Theory of Programming Languages	1	2	3	5	0	1	0	1	2	4	1	3
Human-Computer Interaction	2	5	2	4	2	5	4	5	3	5	1	2
Graphics and Visualization	1	3	1	5	1	1	0	1	1	3	1	3
Intelligent Systems (AI)	1	3	2	5	1	1	0	0	0	0	0	0
Information Management (DB) Theory	1	3	2	5	1	3	1	1	2	5	1	2
Information Management (DB) Practice	1	2	1	4	4	5	3	4	1	4	2	3
Scientific computing (Numerical mthds)	0	2	0	5	0	0	0	0	0	0	0	0
Legal / Professional / Ethics / Society	2	5	2	4	2	5	2	4	2	5	5	5
Information Systems Development	0	2	0	2	5	5	1	3	2	4	0	2
Analysis of Business Requirements	0	1	0	1	5	5	1	2	1	3	0	0
E-business	0	0	0	0	4	5	1	2	0	3	0	0
Analysis of Technical Requirements	2	5	2	4	2	4	3	5	3	5	1	3

Knowledge Areas



Engineering Foundations for SW	1	2	1	2	1	1	0	0	2	5	0	2
Engineering Economics for SW	1	3	0	1	1	2	0	1	2	3	0	0
Software Modeling and Analysis	1	3	2	3	3	3	1	3	4	5	1	2
Software Design	2	4	3	5	1	3	1	2	5	5	1	2
Software Verification and Validation	1	3	1	2	1	2	1	2	4	5	2	4
Software Evolution (maintenance)	1	3	1	1	1	2	1	2	2	4	0	0
Software Process	1	1	1	2	1	2	1	1	2	5	0	0
Software Quality	1	2	1	2	1	2	1	2	2	4	0	0
Comp Systems Engineering	5	5	1	2	0	0	0	0	2	3	0	0
Digital logic	5	5	2	3	1	1	1	1	0	3	0	1
Embedded Systems	2	5	0	3	0	0	0	1	0	4	0	2
Distributed Systems	3	5	1	3	2	4	1	3	2	4	2	4
Security: issues and principles	2	3	1	4	2	3	1	3	1	3	5	5
Security: implementation and mgt	1	2	1	3	1	3	3	5	1	3	5	5
Systems administration	1	2	1	1	1	3	3	5	1	2	3	5
Management of Info Systems Org.	0	0	0	0	3	5	0	0	0	0	0	0
Systems integration	1	4	1	2	1	4	4	5	1	4	0	1
Digital media development	0	2	0	1	1	2	3	5	0	1	0	0
Technical support	0	1	0	1	1	3	5	5	0	1	0	0

Digital Forensics Domain Space



Source: ACM/IEEE Joint Task Force for Computing Curricula (2005), "The overview report covering undergraduate degree programs in CE, CS, IS, IT, SE."

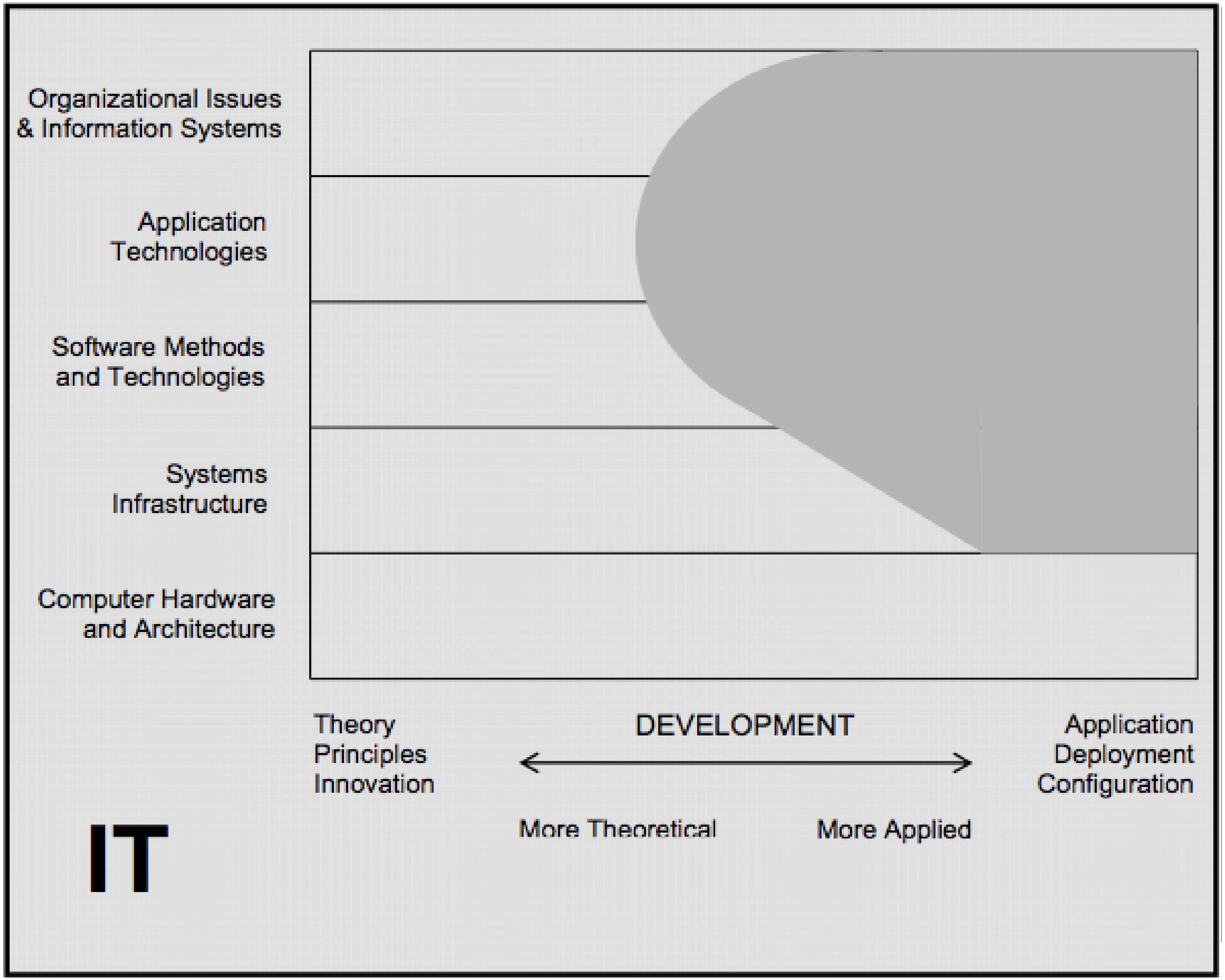
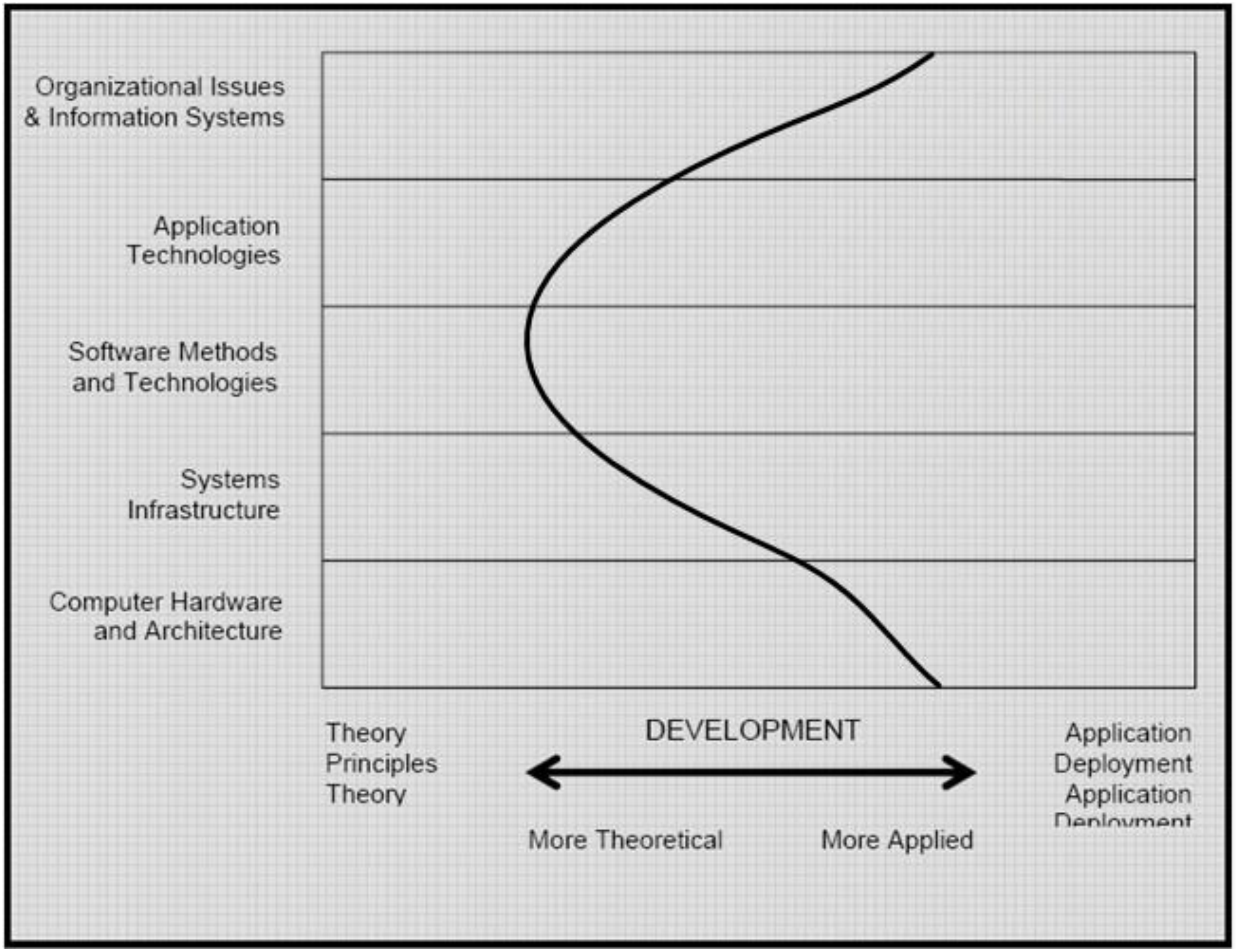


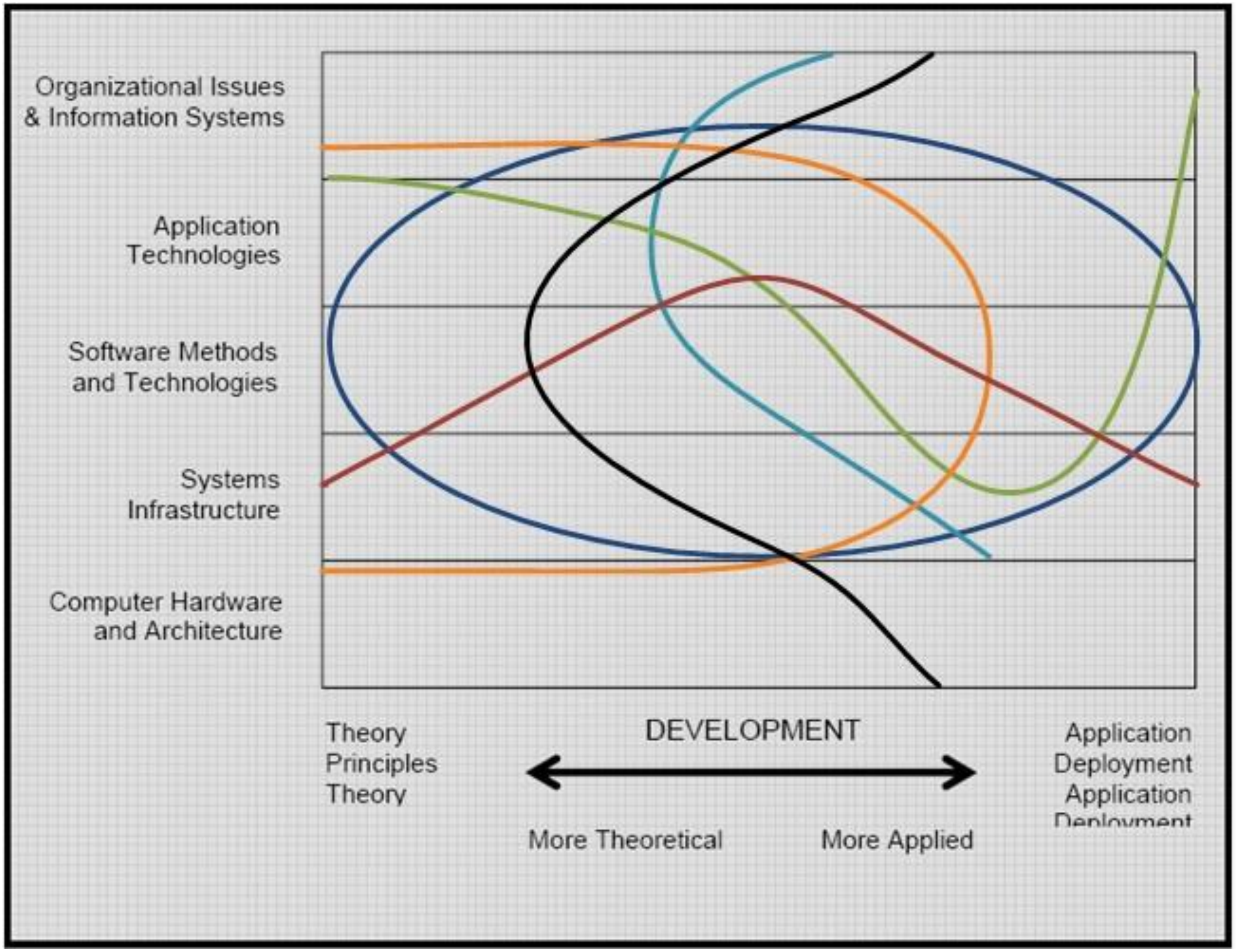
Figure 2.6. Information Technology

Source: ACM/IEEE Joint Task Force for Computing Curricula (2005), "The overview report covering undergraduate degree programs in CE, CS, IS, IT, SE."

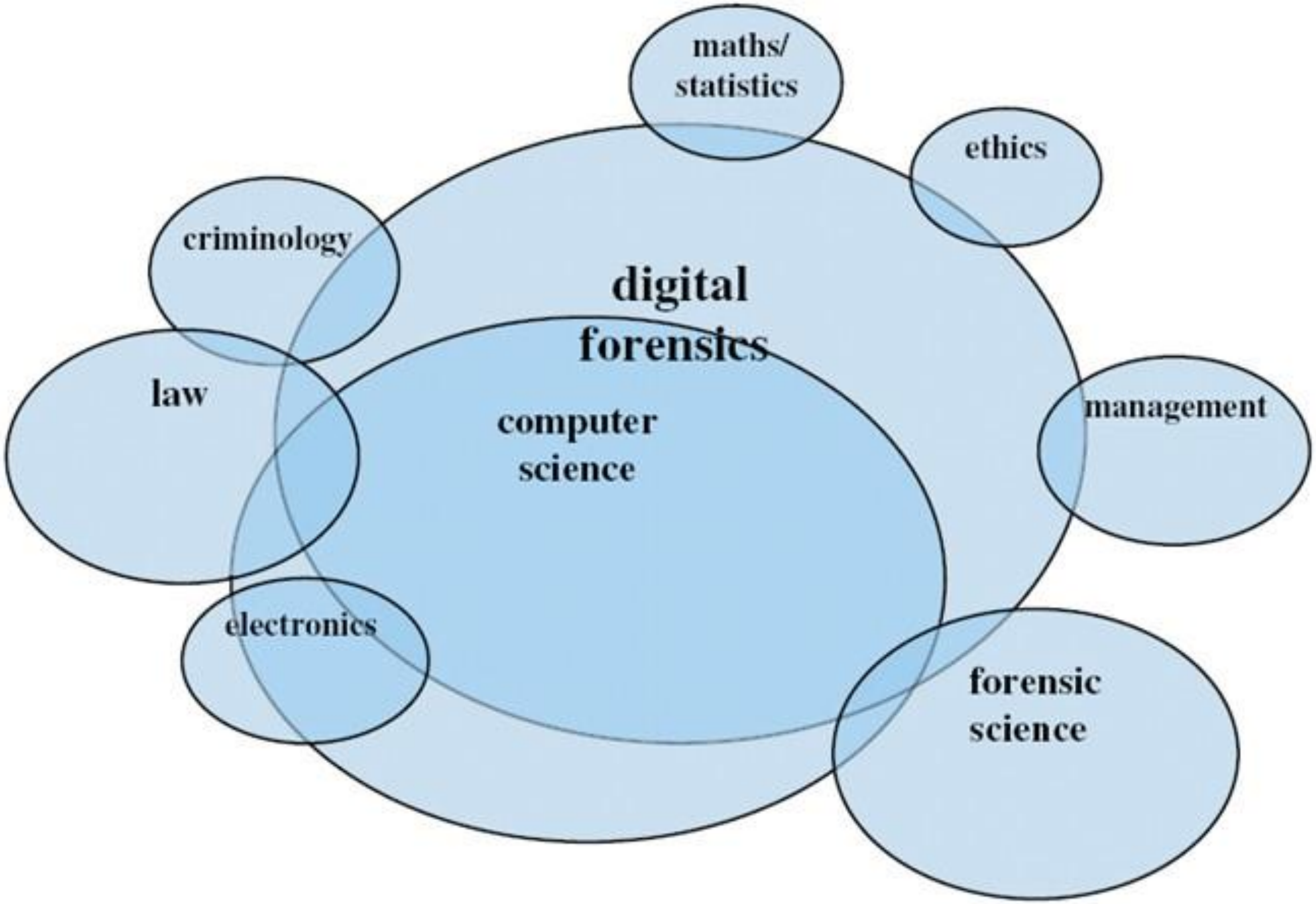
Digital forensics Domain Space



Digital forensics Domain Space


Organizational Issues & Information Systems
Application Technologies
Software Methods and Technologies
Systems Infrastructure
Computer Hardware and Architecture
Theory Principles Theory
DEVELOPMENT
Application Deployment Application Deployment
More Theoretical
More Applied

DIGITAL FORENSICS DOMAIN SPACE



Source:A.D. Irons, P. Stephens, R.I. Ferguson, Digital Investigation as a distinct discipline: A pedagogic perspective, Digital Investigation, Volume 6, Issues 1-2, September 2009

Digital Forensics Education Challenges

- To provide academic researchers with challenging and interesting problems related to digital forensics education
- To develop communities of researchers that can work together to advance the state-of-the-art in digital forensics education
- To develop an education agenda to meet the needs of diverse constituencies who need digital forensics education and training.

- Nance, K., Armstrong, H., & Armstrong, C. (2010). Digital Forensics: Defining an Education Agenda. In *Proceedings of the 43rd Hawaiian International Conference on System Sciences*.HICSS-43.

Digital Forensics Educational Challenges

- *The Unbounded Problem*
  - With the vast number of interconnected systems and users our computing environments do not behave in a predictable way. Considering this chaotic environment, how does one represent in an evidence-lossless fashion, an unbounded data set within finite resources for Digital Forensic purposes?
- *Standards For Digital Evidence*
  - What are the parameters for admissible digital evidence?
- *Embedding Network Forensic Capabilities*
  - Embedding forensics capability to a standard transmission protocol would be helpful in tracing back the origin of a packet. Could such a forensic capability be embedded in a way that the sharing of the forensics data is integrated between the protocol layers?

Digital Forensics Educational Challenges

- *Embedding Systems Forensic Capabilities*
  - What interfaces and data sharing would be required for embedding interoperable evidence collection capability in applications, system software, operating systems and hardware?
- *Demonstrable Forensic Correctness In Tools*
  - Why can we trust a forensic tool? Could “Trusted Forensic Tools Evaluation Criteria” be established?
- *Unified Model Of Education*
  - How would an ideal forensics curriculum look ? What needs to be covered, for how long, what pedagogy would work best, and what would be the pre-requisites?

Conclusions

- Digital forensics is a separate discipline with a distinct academic domain space and a diverse constituency
- There is a need to develop a critical mass of academics concerned with digital forensics
- There is a need to develop a common framework and understanding for digital forensics education

There is a need to provide a forum for digital forensics educators to exchange research, ideas and views.

Future Work

- Examination of the variability and consistency of existing graduate level Digital Forensics courses.

- Comparison of the competencies required in the industry to their perceived importance and time allocated within academic offerings.

- ItICSE 2011 – Working group to develop graduate (MS) level curriculum based on the findings.

Questions

cooper@shsu.edu