

## **Biography: Distinguished Practitioner**

Richard Kemmerer

*University of California, Santa Barbara*

Richard A. Kemmerer is the Computer Science Leadership Professor and a past Department Chair of the Department of Computer Science at the University of California, Santa Barbara. Dr. Kemmerer received the B.S. degree in Mathematics from the Pennsylvania State University in 1966, and the M.S. and Ph.D. degrees in Computer Science from the University of California, Los Angeles, in 1976 and 1979, respectively. His research interests include formal specification and verification of systems, computer system security and reliability, programming and specification language design, and software engineering. He is author of the book, *Formal Specification and Verification of an Operating System Security Kernel*, and a co-author of *Computers at Risk: Safe Computing in the Information Age*, *For the Record: Protecting Electronic Health Information*, and *Realizing the Potential of C4I: Fundamental Challenges*. Dr. Kemmerer is a Fellow of the IEEE Computer Society, a Fellow of the Association for Computing Machinery, a member of the IFIP Working Group 11.3 on Database Security, and a member of the International Association for Cryptologic Research. He is a past Editor-in-Chief of *IEEE Transactions on Software Engineering* and has served on the editorial boards of the *ACM Computing Surveys* and *IEEE Security and Privacy*. He currently serves on the Board of Governors of the IEEE Computer Society and on Microsoft's Trustworthy Computing Academic Advisory Board.

# So You Think You Can Dance?

Richard A. Kemmerer  
Computer Security Group  
Computer Science Department  
University of California  
Santa Barbara, CA 93106  
kemm@cs.ucsb.edu

## Abstract

*This paper discusses the importance of keeping practitioners in mind when determining what research to pursue and when making design and implementation decisions as part of a research program. I will discuss how my 30 plus years of security research have been driven by the desire to provide products, tools, and techniques that are useful for practitioners. I will also discuss my view of what new security challenges the future has in store for us.*

## 1. Introduction

I am really thrilled that you chose me for the Distinguished Practitioner Award. Throughout my research career I have always tried to work on problems whose solution would be useful to others. My approach to research has been one of not just developing new theories, but rather to take the theoretical ideas that I have produced and reduce them to practice. I have always wanted my developments to be used by practitioners. Whenever possible I have tried to provide tools and techniques that others could use to solve the same problems on similar systems or to solve similar problems.

Unfortunately, I do not think that my view is shared by many academic researchers. It is more common for academic researchers to ask “What research can I pursue that will give me a quick route to publishable papers?” or “What can I do to get more funding?”. My approach to research is likely the result of having spent eight years in the trenches as a programmer, system designer, and IT manager before pursuing my PhD and jumping to the academic side.

I would like to say a few words about why I think it is important to keep the practitioners in mind when determining what research to pursue and when making design and implementation decisions as part of a research program. In

my view, the goal of every research project should be that it ends up in use. That is, the research should produce a useful technique, a useful tool, a useful product, or a combination of these three. A question that may be raised is useful to who? For instance, an academic researcher might consider their research effort to have produced a useful product if it resulted in a published paper. I believe that the touchstone here is to ask would a practitioner use my technique, tool, or product? As researchers we should strive to make sure that practitioners are aware of our work (ACSAC is a good venue for this), that our work is relevant to the practitioner (will it make their life easier?), and will the practitioner be able to use it (does it require a special expertise that most practitioners do not have?).

In the next section I will discuss how my 30 plus years of security research have been driven by the desire to provide products, tools, and techniques that are useful for practitioners. At the end of each section I will point out what result (i.e., technique, tool, or product) was produced. I will also try to point out some lessons that I learned along the way. In section 3, I will discuss my view of what new security challenges the future has in store for us.

## 2. Examples From Thirty Years of Experience

### 2.1. Data Secure Unix

Thirty some years ago I started working in Computer Security. My path to get here was different from most. I was primarily interested in Formal Methods and I was looking around for a real application that needed a high level of assurance. At this time most of the formal methods researchers were proving properties about small programs, such as sorting algorithms. Although I believe that having a sorting algorithm work correctly is a good idea, I was looking for something more useful and large. I chose the Data Secure Unix kernel as my application. Data Secure





















