The New Security Paradigms Workshop - Boom or Bust?

Thinking in an Age of Instant Communication; Communicating in a Time of Reflective Thought

Panel Position Statement of Marvin Schaefer
Books With a Past, LLC
2465 Washington Road (MD 97), Suites 3, 4, 5
Glenwood, MD 21738
USA
bwapast@erols.com

1. INTRODUCTION

The basic question this panel has been asked to ponder is: *Have New Security Paradigms Workshops been worth it?* The subtext enquires whether NSPW participants have been wasting time and money[1] by traveling to rustic remote sites to attempt to create new paradigms for addressing information security issues. What has been the Return On Investment (ROI)? Has NSPW had an Impact on the profession or practice?

Holly Hosmer told us she originally conceived of NSPW after thinking about Thomas S. Kuhn's monumental opus *The Structure of Scientific Revolutions*[2], the 200 pages of which were originally published in 1962. This book has become the most often cited work in literature related to the sciences. Ms Hosmer's motivation came from Kuhn's observations that scientific progress and revolution are largely a social process. In essence,

> Paradigms, Kuhn suggests, are the basis of all science. Indeed, what we mean by science are the activities of a group of people ("practitioners") who share a paradigm . Before a shared paradigm exists, Kuhn points out, there is no agreement about what is important and how scientists should proceed. In the absence of a paradigm or some candidate for paradigm, all of the facts that could possibly pertain to the development of a given science are likely to seem equally relevant. As a result, early fact-gathering is a far more nearly random activity than the one that subsequent scientific development makes familiar.
>
> Scientific revolutions, then, are the culmination of a recurrent process in the history of science, according to Kuhn. Paradigms give rise to normal science. At some point normal science gives rise to anomalies, which in turn give rise to a period of extraordinary science. If the outcome of this process is that a new paradigm replaces the old one, a scientific revolution is said to have occurred.[3]

I believe that NSPW has been of high value to its participants and, by extension, to the information security community. I have found a number of presentations to have been particularly beneficial. To name a few:

- Holly Hosmer on applications of Fuzzy Mathematics;
- David Bell and Holly Hosmer on multipolicy systems;
- Dixie Baker on the importance of PCs to finding solutions;
- Bob Blakely on rethinking/redefining the problem;
- Don Welch, Nathan Buchheit and Anthony Ruocco on staging military attacks on cyberattackers;
- Susan Pancho questioning the validity of deliberately perturbing secure protocols and then claiming to have found publishable flaws in the perturbed models;

[1] The chosen term is often euphemised as *resources, funding, grants* or *research stipends.*

[2] In 1962 the University of Chicago press published Kuhn's paper as part of *Foundations of the Unity of Science*, which constituted volumes 1 and 2 of the *International Encyclopoedia of Unified Science.*

[3] Adapted from a review by Dr. Robert E. Wood, Department of Sociology, Anthropology and Criminal Justice

NSPW'01, September 10-13th, 2002, Cloudcroft, New Mexico, USA.

- Jeff Williams, Marvin Schaefer and Doug Landoll on the utility of Pretty Good Assurance;[4]
- and O so many more. . . .

The papers selected above were not all well-received at the time of presentation. Some proved to be very controversial, in fact, and at least one was interrupted so frequently during presentation that only a small portion of the written paper, which all could read at leisure, was ever presented and discussed at NSPW.

At least in the past, NSPW's criteria for selection of papers was much more like that of traditional workshops as opposed to that for conferences and symposia. This has been precisely because NSPW has solicited new ideas, ideas for which not all the details have been worked out (if even identified). Selection had largely been based on:

- Novelty and originality;
- Likelihood that the paper would provide discussion and inspection of underlying concepts and beliefs;
- The likelihood that the discussion would advance understanding;
- The potential to inspire others.

1.1 Literature Citations as a Measure?

My co-panelist, Mary Ellen Zurko, has attempted to address the panel question in terms of objectively identifying the effect of papers published in the *Proceedings* on the industry. Her chosen metric is comparing references to NSPW papers to citations of papers published in other information security conferences and symposia. This scholarly approach is surely one established means of determining the relevance of NSPW to influencing research or to solving (pieces of) the information security connundra.

However one may view the objective statistics as a meaningful metric, I question whether it can or should be applied to establishing the value of NSPW. I believe it is too soon to tell from citations of NSPW papers whether or not the NSPW itself has been worth the effort.

There is also the question of how a published work gets cited when the work appears in a small-tirage publication such as that of the NSPW *Proceedings*. It is true that the *Proceedings of the IEEE Symposium on Security and Privacy* (best known as the Oakland Conference) has also had smallish printings, but many of those papers are now available in reprinted anthologies and CD-ROMs that were published by the IEEE.

But, the Oakland Conference has acquired a mystique of its own for a variety of reasons:

- through promotion by the research funding agencies some contracts have required the submission of interim research papers to the Oakland Conference;
- by cross-referencing of published papers in reports written under research contract to the funding agencies;
- by frequent references in presentations given by identified leaders and experts in the information security research and development community; and
- by its own self-proclamation as being *the première* security conference.

The record should show that I have no doubts about the value of previous NSPW events as *workshops*. Put succinctly, these workshops have given the individual participants more in return than they individually contributed. That is, I believe, the only true measure of the value of a workshop, and in that light, NSPW succeeds admirably.

1.2 Is information Security a Science?

Much of the premise underlying not just the NSPW, but also the question of the effect NSPW has had on information security paradigms tacitly relates to the analogy of paradigm shifts and their effect on established scientific disciplines.

It's fair to ask which portions of our work are part of a scientific discipline. Clearly, the derivation, assessment, and application of cryptologic technologies is as much a science as is any branch of applied mathematics. But, for the most part, I would argue that *information security, in practice, is* not *a scientific discipline*. What we are doing is primarily *engineering*. The differences are discussed in Henry Petroski's remarkable book *To Engineer is Human*.[5]

> The object of a science may be said to be to construct theories about the behavior of whatever it is that the science studies. Observation and experience, inspiration and serendipity, genius and just good guesses — by their presence and absence, in pinches and dashes all can provide the recipe for a scientific theory. . . . Once a theory has evolved, perhaps from a half-baked idea to a precise and unambiguous statement . . . the scientific method may be used to judge the success or failure of a given theory or the relative merits of competing theories. . . . A scientific hypothesis is tested by comparing its conclusions with the reality of the world as it is. . . . Yet all it would take would be a single . . . [instance of the hypothesis failing] to make [it] categorically false. . . . Engineering design shares certain characteristics with the positing of scientific theories, but instead of hypothesizing about the behavior of a given universe, . . . engineers hypothesize about assemblages of [materials] that they arrange into a world of their own making. . . . Now should [a bridge built

[4] This presentation appears to have anticipated the Common Criteria.

[5] *To Engineer is Human, the Role of Failure in Successful Design*, St. Martin's Press, 1985, chapter 4.

> under this hypothesis] collapse suddenly under no extraordinary conditions . . . there would be no doubt in anyone's mind that the original hypothesis was incontrovertibly wrong. The process of engineering design may be considered a succession of hypotheses.

Engineers traditionally perform *compromises* to accommodate the need to achieve *tradeoffs* among available materials to optimise results. A scientific or mathematical model of a system's *secure* operation would need to show that the effects of *every* possible operation would keep the system in total compliance with its security conditions. This concept has been called, in modified form, the *reference monitor concept*.[6] McLean showed that the very act of representing such a model by using state transitions is fraught with potential logical peril.[7] This important *scientific* consideration aside, the act of monitoring and refereeing *every* microstate transition on a computer system or network would be a practical impossibility.[8]

So a form of "chunking" has always been the ingenious security engineering compromise. A hypothesis is built that if implemented, results in a model that:

- manages a subset of the set of system micro-operations T,
- defines a subset of a system's active agents S,
- defines a subset of a system's information containers O,
- considers a subset of a system's potential state space $< T,\ S,\ O >$, and
- abstracts a simplification of the security requirements that are to be imposed over identifiable events that take $< T,\ S,\ O >$ into $< T,\ S,\ O >$

and produces an adequate solution to the information security problem.

Only the passage of time and the compilation of huge numbers of experiments will serve to support or undermine confidence that the chosen engineering compromises and tradeoffs have been adequate to satisfy the formulated requirements. To date, experience has shown that the problem continues to become more complex and the validity of the "solutions" become more quickly eviscerated. And so, experimentation continues and solutions remain elusive.

Indeed, many "promising" approaches have been taken over the last three decades. Some appear even to have brought about short-lived paradigm-shifts. Many of these have been taken as blessèd panacea. But along have come overwhelming changes to the engineering solutions' definitions and assumptions (distributed computing, multiprocessors, proliferation of interpreters for active data, personal computers, the Internet, dissemination of hacking tools, pervasive cryptanalytic tools, the G4, Free Kevin, etc.).

[6] James P. Anderson, *et al.*, "Computer Security Technology Planning Study," vol 1, ESD-TR-73-51, ESD/AFSC, Hanscom AFB, Bedford, MA, October 1972.

[7] John McLean, "Reasoning About Security Models," *Proceedings of the IEEE Symposium on Security and Privacy*, Oakland, 1987, pp 123-131.

[8] This would probably a theoretical one as well because of expected self-referentiality.

2. PERCEIVING THE TIME FOR CHANGE

Is there a double standard here? If the effectiveness of NSPW is being questioned, should one not also question the effectiveness of all of the information security conferences to date? Should not one ask what the effective existing paradigm is? This question was effectively raised by Steve Greenwald at NSPW 1998 in his "Discussion Topic: What is the Old Paradigm?"

2.1 Background

Research on the "computer security problem" began in the mid-1960s with the publication of the U.S. Defense Science Board's Ware Report,[9] a few classified meetings within the U.S. intelligence community, and with the development of System Development Corporation's ADEPT-50 multilevel secure prototype operating system. An early capstone state was reached by 1975 due to additional research conducted at Case Western Reserve University, RAND Corporation, and at the Air Force- MITRE-Honeywell project that led to the Bell-LaPadula security model and the MULTICS operating system. Indeed, now that everything but the details had been hammered out, success was asserted and research moved on to the next big problems: multilevel network security and multilevel database management security. By 1984, security research had become such a dull topic that secure system/secure product development had been largely transitioned to mainstream industry. With the growing feeling, particularly amongst the echelons of senior government officials, security research moved into new areas: perfection of formal methods, secure applications, mutual suspicion, product evaluation methodologies, public key cryptology, etc.

Failings in security technology began to become increasingly visible:

- Discretionary access controls could always be exploited by Trojan horse attacks;
- Multilevel secure operating systems were vulnerable at the highest security levels to penetration attacks mounted from the lowest security levels;
- Covert channel analysis, once touted as a ridiculous pursuit, had revealed the existence of indetectable and unconstrainable leakages that could be exploited at hundreds of kilobits per second;
- The technology of the computer virus became public knowledge.

[9] Willis Ware, ed., "Security Controls for Computer Systems," AD-A076-617/0, (CONFIDENTIAL), the RAND Corp., Santa Monica, CA.

The mantra from IBM's Bob Courtney, Harry DeMaio, Stan Kurzban, and Bill Murray was echoed by the National Security Agency's Hilda Faust and its chief information security official Bernie Peters. They chanted: "Security failures occur not because of technical exploitation of security flaws, they occur because of bad management practices by system and facility administrators.

So well before the founding of NSPW in the early 1990s, information security technology had reached the point where its practitioners had largely declared success. However, many sceptics and critics were finding themselves to be more generally heeded than the established security guru population. Why? Well, simply put, everything about security was too slow, too costly, and too impotent to be of any value. There had not yet materialised any groundswell of public demand for secure products. Companies that had been developing high-assurance systems[10] canceled projects for a myriad of reasons, until only government- funded projects remained targeted at these levels. And, governments, whilst praising the virtues of the TCSEC, ITSEC, and ultimately other standards continued to use and procure only securityless low-assurance products. Indeed, the Director of the National Security Center refused to use any evaluated C2 or higher product on his own workstations.[11]

So the state of the art certainly was ripe for a scientific revolution that would bring in a new scientific paradigm. Unfortunately, there was essentially no science against which to revolt. . . .

2.2 The Influential Conferences

Before 1979 there were no conferences dedicated exclusively to computer or information security. There had been several invitational workshops, mostly classified or that never published proceedings. Noteworthy amongst the unclassified workshops were the Workshops on Computer Security and Audit, sponsored by the National Bureau of Standards. It was from these workshops that the initial public formulation of draft security assurance, architecture and evaluation standards first appeared in print.[12]

In 1979, Steve Walker (US DoD) and Jim Burrows (NBS) introduced the first of a series of Symposia on the DoD/NBS Computer Security Initiative. These irregularly-scheduled symposia were held at NBS and were intended to be educational, bringing together researchers, practitioners and potential users from government, industry and academia. The published proceedings consisted of speakers' visual materials and occasional typed papers by the invited speakers. These symposia ultimately grew to become the National Information Systems Security Conference, which essentially published only papers that had been formally refereed. Starting as single-track symposia, the evolution from symposium to conference also led to multiple concurrent sessions and thematic "tracks".

In 1980, the first of the major research symposia occurred. This was the IEEE Symposium on Security and Privacy, conducted annually thereafter in Oakland and consisting of strictly-refereed papers and panels covering topics in cryptology, computer and network security, and formal methods. This symposium has generally limited attendance to fewer than 400 souls, and has favoured selection of papers having a strong original research flavour, although the program committee occasionally selected practical papers. The main sessions of this symposium are single-track, with a single paper or panel being given at a time.

Additional information security conferences subsequently developed, including the ACM Security Conference, the ACSAC, Security Foundations Conference, IEEE Working Groups in Security, Safety, Database Management Security, Fault Tolerance and Security, CRYPTO, EUROCRYPT, ASIACRYPT, National Computer Security Conference, Black-Hat, DEFCON, SANS, *etc.* These conferences range from offering formally refereed papers all the way to offering non-refereed invited papers and tutorials.

This is all swell, but for one minor nit. While many papers from these long- standing conferences have been cited in the literature, it is to be noted that security posture of most computer systems today is far weaker than ever before. Largely, this is because of the convergence of two major events: (a) the progress made in developing, and making readily available, attack and exploitation techniques and toolkits that can be used effectively by unskilled miscreants and (b) the abandonment of attempts to design and implement systems with architectures designed to defend themselves against misuse.

3. TIME NEEDED FOR CHANGE

We live in a time of nearly instantaneous communication. Nothing happens as rapidly as is expected; things just always take longer than optimists[13] expect. As the speed of computing or communicating increases, so also does public impatience.

This impatience can be witnessed frequently in mass public behaviour. Investors become frustrated when changes in the short-term interest rate do not instantly effect the stock market. Consumers become impatient when prices at the fuel pump are not immediately changed to reflect changes in the wholesale price for raw petroleum or when newly announced medical advances do not become instantly available at their local chemist's.

Funding agencies have become very impatient with the lack

[10] *E.g.*, systems targeted at the A1 or higher levels of assurance

[11] He gave numerous reasons for his policy: the systems were not user friendly, too hard to learn, too slow, not supported by good maintenance, and too costly. He observed that with their C2 features turned on, the systems essentially ground to a halt (particularly if security audit features were turned on). Although the intelligence community had sponsored the Compartmented Mode Workstation, it also was not used, generally for the same reasons plus some lingering concern for the strong criticism CMWs had received by certain outspoken members of the security research community.

[12] These workshops were held in Gaithersburg and in Miami Beach.

[13] Innovators, of course, are largely optimists

of a solution to the information security problem. The *appearance* that progress is being made may be just as important as the actual making of progress. I believe this is the reason for the popularity of stopgap security add-on products such as firewalls, virus scanners, Java sandboxes, formally verified specifications or protocols, and other pseudoscientific placebos and elixirs. All of these serve a limited defence purpose, and some are reasonably powerful. Many of these ideas were partially-birthed at NSPW workshops!

But none solves the problem. Since the problem may well not be solvable, the amount of time required will remain an open question.

4. RÉSUMÉ

Because it is a workshop, NSPW has always drawn its principle benefits from and given them back to, its participants. NSPWers have not left their thinking behind when they departed from the resort but instead have continued communicating with one another and with their colleagues at work about the ideas that provoked them during their three days together.

Several of the ideas advanced at NSPW have shown up in doctoral dissertations, in conference papers, and in new products though it is impossible to trace their unique lineage. It is a sad commentary on our profession that every few years its past is recreated. Largely this is because computer security "professionals" do not always read the literature that they cite, as has been seen repeatedly in references to the Bell LaPadula model, and far too many other papers that I have refereed for Oakland and other prestigious conferences and symposia. This has resulted in numerous reinventions of errors of the past. In a letter to Hooke, Sir Isaac Newton who is generally credited as having set several new paradigms in the sciences, wrote the following prophetic remark.

> What Des-Cartes did was a good step. You have added much several ways, & especially in taking ye colours of thin plates into philosophical consideration. If I have seen further it is by standing on ye shoulders of Giants.[14]

REMERCIEMENTS

I should like to express my gratitude to Steve Greenwald and Mary Ellen Zurko for numerous probing discussions that provoked my participation in this panel when it was initially proposed, and to Holly Hosmer who first acquainted me with NSPW's principles O so long ago *quand j'étais viellard.* My participation was facilitated through the generous efforts of Steve, mez, John McHugh, and Cristina Serban. Finally, I should like to thank Victor Raskin for so graciously taking the reins as Publication Chairman, and to all the participants who were able to concentrate on NSPW during the perilous times in which we met. *Merci à tous!*

[14]Newton to Hooke, 5 Feb. 1676; The Correspondence of Isaac Newton, Volume I, page 416 .