The New Security Paradigms Workshop - Boom or Bust? A Panel

Steven J. Greenwald
Independent Consultant
2521 NE 135th Street
North Miami, Florida 33181
USA
sjg6@gate.net

ABSTRACT

Has anything actually been accomplished by the New Security Paradigms Workshop since its inception in 1992? If so, what? This, in a nutshell, was the basis of our panel. We had three high-profile NSPW groupies as panelists: our illustrious founder Hilary Hosmer who gave a passionate ponderment of the past 8 years, a perspective from Mary Ellen Zurko who entered NSPW during the middle of its current lifetime (1996) and has authored many reviews of NSPW for CIPHER, and some punishing comments by Marv Schaefer. I also entered the NSPW community in 1996, and was the panel chair in what was a very interactive panel. We had a view from the early days and a view from the more mature days of the ten year old New Security Paradigms Workshop.

What did we find out? Were the past years of NSPW wasted? Or did they result in some of the best ideas to hit the information security field? Or something in between?

In either case, where should we go from here?

The format of the panel was simple. Each panelist gave a brief presentation with the workshop participating in its usual collegial style, with the panel chair to keep things on track.

After the workshop, the original panel charge was revised to reflect and add the comments of the workshop attendees.

1. INTRODUCTION

Since the beginning of the New Security Paradigms Workshop (NSPW) in 1992, two computer generations have occurred. During that time, NSPW has been a fertile substrate for radical ideas, unfinished works which benefit from the NSPW environment, and the cross-breeding of other disciplines with information security. The result is a brainstorming session unparalleled in the security community.

But is it worth it? Has anything worthwhile, or of even moderate interest to the information security community emerged? Is the NSPW method truly effective for advancing new ideas, challenging old ones, and encouraging new authors? Or is it a waste of time and effort?

Enough time has passed that the NSPW "experiment" can now be evaluated. The results from the past two generations of NSPW stand as evidence to be used to indict it as an experiment that has failed, or to confirm that it is a success.

2. DRAMATIS PERSONAE

It is desirable to have panelists who keep abreast of current research and deployment issues in the broader security community and yet hold strong views regarding NSPW. Each panelist has provided a position statement. These statements have highlighted some of the significant topics from the history of NSPW. We looked at NSPW papers that have proven prescient, seminal, way off base, and those that still have potential. When all the panelists were done presenting their positions, the debate via workshop participant questions and answers and panel participation commenced in earnest (there was debate during the presentations as well). Workshop participation provided probing questions and perspectives on the positions of the panelists.

The names and qualifications of the panel follow.

- Hilary Hosmer is the founder of NSPW, the past general and program chair, and an author. She is currently president of Data Security, Inc., working in rapid risk analysis, visualization, and privacy. Her NSPW contributions are many. They include multi-policy paradigms that critiqued the Orange Book and proposed the need for handling more than one security policy (due to policy differences in interconnected political domains). Another one challenged the basic assumption of the Red Book that the network administrator had to know the exact network configuration, as opposed to the then-emerging need for managing

dynamic networks. Ms. Hosmer wonders the following. Have we really accomplished anything? Which paradigm over the past nine years has been the most important? Where should we go from here?

- Mary Ellen Zurko first joined NSPW in 1996 as an author (her seminal paper on User Centered Security was presented then). She is a past program chair, and the current general chair. She is currently a Security Architect at Iris Associates responsible for active content security in Lotus Notes and also chairs e-commerce tracks for several Web and Internet conferences. Her early NSPW work on User Centered Security was presented in a more mature form at the 1999 S&P.

- Marv Schaefer was present at the second NSPW, was very active in the organization as publications chair, was an author, and is a long-time participant. He has been very many things in life; currently he is an antiquarian bookseller. His contributions are in areas such as the need for integrity over confidentiality, defending against the abuse of authority rather than of break-ins (*i.e.*, the misuses of existing mechanisms in authorized ways goes much farther than trying to break them). While Marv also believes in the fact that Formal Methodists were off-base and irrelevant, his NSPW research also focused on how analysis and defenses would better be focused on the problems that need to be solved (*i.e.*, the attacks that work) rather than the toy ones that formal methods found useful (*e.g.*, detecting violations of the *-property in abstract from specifications that are, at best, only coincidentally implemented in code).

- I chaired the panel. I have been involved with NSPW starting in 1996 as an author, am a past program chair, past vice chair, and am this year's general chair. As an independent consultant and adjunct professor in information systems security, my research interests include Role Based Access Control, decentralized security, User Centered Security, Resource Based Security, proofs of NP-completeness of various security properties, and covert channels.

The choice of panelists was, of course, quite deliberate, being a mix of the first and second generation NSPW attendees. The panelists helped to highlight the evolution of the workshop.

3. THE DESCENT OF NSPW

NSPW has had an interesting evolution! Starting with "refugees" from Franconia, IEEE WG 11.3 (DBMS), Oakland, and the Applications conference (as well as some non-refugees), NSPW has evolved into a more mature form while still accepting radical and semi-radical contributions. In the words of Marv Schaefer commenting on the early days of NSPW:

> Papers from students started flowing in, but at first the papers were from attempts to get an idea in one of the "Mature Conferences" and,

for one reason or another, finding that NSPW was a better place for the paper. So Holly Hosmer's attempts to go for fuzzy sets and for adaptable policies were a natural rejection for the other conferences and a natural fit with NSPW – not yet publishable in a "refereed responsible scholarly journal"[1] but ideal for a group like ours because the author ends up, when she wins, learning something so that the idea can be refined for the future.

3.1 "In The Beginning . . ."

The following were a few of the issues addressed at the very first NSPW.

- Computer security paradigms should address the needs of non-U.S. Department of Defense users.

- In 1992 current approaches to evaluation and certification focused exclusively on trusted systems. The idea of making evaluation and certification of trusted products *user driven* was proposed and discussed.

- Sociotechnological aspects of computing were noted as being ignored by the mainstream security paradigms, resulting in security that was widely supported but poorly defined. Enterprise modeling was proposed as one solution towards realistic policies. It was also noted in this context that formal methods cannot replace the basic understanding of what is needed to make a system secure.

- The idea was advanced that it may not be possible to build a completely secure system, as the current dogma held.

- Pragmatic issues, such as the fact that training users "in the trenches" in how to apply trusted software development methodologies was largely ignored at that time.

- Paradigm shifts were predicted by the participants. Among them were the following.

  - Subject-object level security shifting to application level security.

  - Centralized hierarchical systems shifting to decentralized interoperable networks.

  - The reference monitor paradigm shifting away from the "guard" model to a proxy model to address integrity and availability along with confidentiality.

  - The idea that it is possible and desirable to design a system right the first time shifting to systemic flaw reporting and correction.

  - The idea that polices are understood shifting to enterprise modeling of sociotechnological aspects of computing.

---

[1]Lest anyone get the wrong idea, NSPW is peer-reviewed and NSPW submissions are rigorously refereed – SJG.

Are these worthwhile ideas? What has evolved since? Can we say that NSPW has had *any* impact on the field or community since its inception? To help answer these questions, I present some of the latest ideas to emerge from NSPW.

3.2 Post Post-Modern

- The idea that defensive information warfare will *always* fail, and that *offensive* information warfare is necessary.

- Optimistic security as an access control paradigm, where in certain situations (*e.g.*, hospitals) users are permitted to violate standard access control paradigms in the interests of safety.

- An examination of the way market forces may drive the use of protection profiles in the Common Criteria.

- Paradigm shifts in protocol analysis that involve changes in assumptions about environment and context.

- A prolepsis on Trojan horse based integrity attacks. Does current practice takes the tacit and pessimistic view that the Trojan horses problem is unsolvable? If the answer is "yes," (as seems to be the answer in the prevailing paradigm), a case was made that this view is in principle, wrong, and the problem is in fact, solvable.

- A discussion as to the nature and definition of the old security paradigms due to the view that it is necessary to define the old paradigms before the novelty of "new" ones can be considered with anything approaching scientific rigor.

- A new system integrity model that is implementation independent.

- A new method of downgrading that uses decision trees to avoid the inference problem.

- Since bugs are ubiquitous, a new paradigm called *bug tolerance* that enhances the survivability of flawed systems *post hoc*.

4. STOCKING UP ON BANDAIDS AND DILUTE IODINE

During the organization of this panel, Marv Schaefer stated the following.

> At the time when the NSPWs started, there was an established set of Hallowed Principles and Practices (HPP) that were nearly universally accepted and not followed because we all knew that trusted technologies were effective but not efficient. HPP were being challenged at NSPW meetings in a majority of the papers and discussions, and projections of problems and needs yet to be voiced were put forward along with a number of proposed means of approaching their solutions. Since then, alas, the prognostications came to pass: Internet Security has come to be synonymous with

Bandaids and dilute Iodine (AKA Firewalls and virus scanners). Trusted operating systems and Network Security solutions have been replaced by cryptography with weak key distribution or key secrecy practices that run in easily penetrated operating systems that have been misconfigured by untrained system administrators. Information Assurance appears to be an appeal for Tinkerbelle (and her friendly security færies) to run SATAN and sprinkle SecurityDust^{TM} (Patent Pending) on bad configurations.

The above should convey a sense of the charge to the panelists. Our intent was to be both self-critical and self-congratulatory. Both castigated, and defended. Workshop member's interest and participation was high, and the panel was lively and provocative, while serving the useful role of helping to determine and define NSPW's proper place.

In my role of NSPW organizer, I am sometimes asked, "Is NSPW an honest and serious workshop, or is it just a place to publish whacko half-baked stuff that no one else wants?" When the smoke cleared, we had an answer to that question!

5. COMMENTARY EXPERIMENTATION: GOING THROUGH SUBCOOL MUTATION

What follows are some of the comments that the NSPW participants had regarding issues brought up during the panel. They are in no way complete. I think it is safe to declare that everyone at the workshop participated in the panel.

In what follows I am perhaps stealing a bit from what is rightfully the domain of other panelist's positions, but I wish to give a holistic view of the entire panel discussion. I apologize to my fellow panelists if I have stepped on their toes, and I apologize to any readers who are offended at any redundancy that may occur. But I feel strongly that it is important to try to convey a sense of what NSPW is like to those that have never attended, and to also document as closely and totally as I can the interaction and *mutation* (if I may use that word) that occurred during the panel's brainstorming session and is so typical of NSPW.

5.1 Metrics alá Mez

Victor Raskin wanted to know how many of this year's participants were advising graduate students. Six people raised their hands. He thought that it was possible that the main source of paper citations came from advisors' graduate students who naturally cite their advisor's papers. Since NSPW has less than the traditional amount of academic advisors (since we actively encourage graduate students and industry personnel to attend) he thought that this would naturally skew Mary Ellen Zurko's (AKA Mez) citation metric. Victor also has heard that many universities are considering dropping citation indices as a criterion for promotion because the data are worthless. I'm certain that Mez has more to write about this in here position paper.

Bob Blakley speculated that one reason his truly outstanding and oft-quoted 1996 paper, "The Emperor's Old Armor" isn't cited more often is because he doesn't have a website and therefore the paper isn't available electronically. However, I have recently discovered that the paper is available (for a fee) from the ACM Digital Library (as are all NSPW proceedings/papers). Note that many academics get unlimited access to this library, and it is certainly worth paying to get a copy of Bob's paper in my opinion.

Carol Taylor asked if there are any good measures of a paper's influence other than citations. Good question!

5.2 Influence or Influenza?

John McHugh responded to all of this by asking a very profound question: what subfields have we initiated in the literature? For example, Fred Schneider's work on inline reference monitors, and Stephanie Forrest's work on immune systems approaches for intrusion detection are two examples that came from NSPW.

Several people then noted that work which makes its debut at NSPW isn't usually cited. Instead it is the later more "polished" works that appear in other places that are cited. I think that the list of topics from the first NSPW in section 3.1 bears this out.

Ken Olthoff wondered whether NSPW's influence on the attendees is more significant than influence on others. In other words, do the NSPW attendees go out and "proselytize?" An interesting question! Many people confessed that they did, and I know that I do.

Marv Schaefer pointed out that during the workshop itself, most of the insights come from the sessions themselves. But elsewhere at other conferences and workshops most of the insights come from the breaks. This is a profound insight. In my opinion, this is one of the distinguishing features of NSPW, and a great *desideratum*. We truly are productive and not just another group that only "networks."

5.2.1 An Interesting Diversion

Victor Raskin went off on a little tangent (by the way, this is very typical of how NSPW works). He said he believes that computer science doesn't have to be science, because it is really just applied mathematics. This is also a topic that was on my mind and I agreed to a point, but I theorize that it is neither science nor engineering, but something altogether new in the taxonomy of human knowledge. We are distinguished by the notion of "policy" in information systems security for example, and computer science is distinguished by the notion of automatic decision making. This is probably grist for another paper. I include this diversion to show how NSPW acts to spin-off ideas. Now back to the main discussion.

Bob Blakley commented that the value of NSPW is that it promotes the idea that doubt is okay. Prompted by this, Mary Ellen Zurko observed that it is easy to get depressed in a field in which the performance criterion is perfection.

Victor Raskin noted that he has essentially been "accred-

ited" into the security community by NSPW. This means we are an avenue for multidisciplinary entry into security. Stephanie Forrest was also introduced into the security community by NSPW.

Bob Blakley suggested that even the *existence* of a conference with the name "New Security Paradigms Workshop" may goad other conferences to try harder and to broaden their perspectives.

It is especially interesting to note that Bob made this comment a little later on in the strict chronology of the discussion. I placed his remarks here because I thought it was appropriate. This points out one of the other characteristics of NSPW: ideas and comments happen so fast and furious that there are sometimes delayed responses that are made after the issue has already passed. This might happen because it just pops into the participants mind at that later time, but usually happens because sometimes it is hard to get a word in! Plus, Bob was acting as scribe for this discussion which is a very difficult job.

5.3 Moths to the Flame or Travelers to the Stars?

Ellen McDermott asked why people came to the workshop. The unanimous answer for first timers was simply to get their papers published. Sami Saydjari answered Ellen's question by saying that many established conferences will not expand their existing focus and will not accept papers out of the traditional categories.

I countered Ellen's question with a different question: why do people come back even when they have no paper to publish? For example, Simon Foley mentioned that he has published at Foundations, Oakland, and NSPW, and keeps coming back. John McHugh observed, and many agreed that it was because of the stimulation offered at NSPW. Cristina Serban said that it was because she enjoys being in a group of *humans* discussing technical issues where there are no battles.

Ellen McDermott suggested that we might want to expand a little in the direction of practitioners as opposed to academics, industry types, *etc.* John McHugh thought that we would be very open to discussion proposals of this type and many agreed, myself included. Although Mike Williams wondered if we could get people from this background who would really contribute to the discussion.

5.4 Interaction

Bob Blakley suggested that after watching people struggle with ideas here, and going to other conferences, he is disappointed with the low level of new conceptual content of many other conferences and the predictability of many results. Most attendees seemed to agree with him, and I know I certainly do.

We wrapped up with a comment by Mike Williams, who said that he finds the interaction quality at NSPW higher than anywhere else. Well said Mike!

110

6. BOOM OR BUST?

Based on the other panelists statements and on the discussion, I have come to the conclusion that NSPW is an unqualified boom. "Metrics" of success are difficult, as the panel showed, but there can be no question that NSPW is fulfilling its role as being a fertile breeding ground for new ideas that might not be accepted at more orthodox conferences.

One of the perceived problems is that NSPW articles don't appear to be cited as often as they should, assuming we are presenting new and seminal work (which history shows we are). But as was pointed out, most of the ideas that spring from NSPW are cited in later incarnations at more mainstream conferences. In addition, the "citation mill" doesn't work as well with NSPW due to our small size and mix of students and non-academics.

Also, it is impossible to quantify or qualify the unique brainstorming environment of NSPW, where the atmosphere is never confrontational and is, instead, helpful in the extreme. This is especially helpful for new ideas.

If there is a flaw in the NSPW system it is one of publicity. Perhaps we need to do better to get the ideas presented at NSPW more into the mainstream. Part of this problem stems from the fact that our proceedings are printed and distributed after the workshop.

I think it is clear that NSPW has been a huge success over the past 10 years, and gives every indication of being so for the next decade.

ACKNOWLEDGMENTS