Themes and Highlights of the New Security Paradigms Workshop 2003

O. Sami Saydjari
Cyber Defense Agency
ssaydjari@CyberDefenseAgency.com

Carla Marceau
ATC-NY
carla@atc-nycorp.com

Abstract

This panel highlights a selection of the most interesting and provocative papers from the 2003 New Security Paradigms Workshop. This workshop was held August 2003 - the URL for more information is <http://www.nspw.org>. The panel consists of authors of the selected papers, and the session is moderated by the workshop's general chairs. We present selected papers focusing on exciting major themes that emerged from the workshop. These are the papers that will provoke the most interesting discussion at ACSAC.

Panel Theme

This panel presents a selection of the best, most interesting, and most provocative work from the New Security Paradigms Workshop 2003. For twelve years, the New Security Paradigms Workshop (NSPW) has provided a productive and highly interactive forum for innovative new approaches to computer security.

NSPW is an invitational workshop of deliberately small size, in order to facilitate deep, meaningful discussions of new ideas. Authors are encouraged to present work that might seem risky in other settings. All participants are charged with providing constructive feedback. The resulting brainstorming environment has proven to be an excellent medium for the furthering of "far out" and visionary ideas.

Our philosophy is to look for significantly *new* paradigms and shifts from previous thinking, and facilitate the debate within a constructive environment of experienced researchers and practitioners along with newer participants in the field. In keeping with the NSPW philosophy, this panel challenges many of the dominant paradigms in information security. You can definitely expect it to be highly interactive; in the NSPW tradition, look forward to lively exchanges between the panelists and the audience. So come prepared with an open mind and ready to question and comment on what our panelists present!

Past NSPW conference panels have dealt with a wide variety of subjects including the following: software engineering of secure systems; penetration tolerance; new directions in cryptography and steganography; alternative models of trust and authorization; user-centered security and end-user defenses; new models for securing "boundless networks"; deficiencies in traditional definitions of security, secrecy, and integrity; security in PDA devices; attack modeling; offensive information warfare; the effectiveness of biometrics; mechanisms to combat email spam; and a framework for data privacy management

The last NSPW panel was held at ACSAC 2002 and was well received, very lively and highly praised by the audience, ACSAC organizers and panelists alike.

Here are some of the latest ideas to emerge from NSPW, aside from those you will hear from the rest of the panelists.

- 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. Protocol analysis paradigms enlarging their assumptions to include environment and context.
- A case was made that we must reconsider our approach to information security from the ground up if we are to deal effectively with the problem of information risk.
- 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.
- A new approach to helping applications defend themselves, while disarming hosts via the use of filters.
- Since bugs are ubiquitous, a new paradigm called bug tolerance that enhances the survivability of flawed systems *post hoc*.

The panel will consist of four authors of papers selected by the NSPW 2003 General and Program Chairs, and it will be chaired by the general chair. After the panel chair's introductory remarks, each panelist will then give a 10 to 15 minute presentation. The floor will then be opened for audience questions and discussions. This format has worked extremely well in the past, and we plan to continue the tradition.

So come to our panel and discover this year's **new** paradigms! You'll either immediately like them or dislike them - and you'll get the chance to say so!