Highlights from the 2005 New Security Paradigms Workshop

Simon Foley, University College Cork, *Moderator*
Abe Singer, University of California at San Diego, *Moderator*
Michael E. Locasto, Stelios Sidiroglou and Angelos D. Keromytis, Columbia University
John McDermott, Naval Research Laboratory
Julie Thorpe, Paul van Oorschot and Anil Somayaji, Carleton University
Richard Ford, Mark Bush and Alex Boulatov, Florida Institute of Technology

Abstract

This panel highlights a selection of the most interesting and provocative papers from the 2005 New Security Paradigms Workshop. This workshop was held September 2005 - 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.*

1. Panel Theme

This panel presents a selection of the best, most interesting, and most provocative work from the New Security Paradigms Workshop 2005. For fourteen 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!

2. Panel Format and Papers

The panel will consist of four authors of papers selected by the NSPW 2005 General and Program Chairs, and it will be chaired by the general chair. Following are abstracts of each paper selected for presentation

2.1. Speculative Virtual Verification: Policy-Constrained Speculative Execution

The ability for computing systems to autonomously detect and correct faults and vulnerabilities would greatly improve their stability and security. The job of processors has long been to simply execute code, and getting them to do exactly that at high levels of performance has been the focus of research and industry development. As a result, security is not integrated into the fabric of execution.

This paper advocates modifying general-purpose processors to (a) provide implicit supervision functionality, (b) export a policy-driven monitoring mechanism, and (c) provide the foundation for an automatic response capability via instruction stream rewriting.

We propose *speculative virtual verification* (SVV), a set of architectural components that provides a basis for such systems by speculatively executing the entire instruction stream. In much the same way that a superscalar processor speculatively executes past a branch instruction and discards the mis-predicted code path, we propose that processors operate on the in-

struction stream in two phases. The first phase executes instructions, optimistically "speculating" that the results of these computations are benign. The second phase makes the effects of the speculated instruction stream visible to the OS and application software layers and potentially rewrites the instruction stream if it has been deemed harmful.

2.2. Visual Security Protocol Modeling

This paper argues that the existing model-driven architecture paradigm does not adequately cover the visual modeling of security protocols: sequences of interactions between principals. A visual security protocol modeling notation should be event-based, compositional, comprehensive, laconic, lucid, and well-defined. We can say informally that: event-based visual modeling focuses on interaction patterns and avoids details of internal computations; compositional modeling languages allow protocol models to be built from submodels that clearly correspond to the principals; comprehensive modeling languages can define all traces of a security protocol with a single model; a non-laconic model has more than one visual token representing the same modeled object; a non-lucid model has more than one modeled object represented by the same visual token; a well-defined language has a formal syntax and semantics.

Candidate visual modeling notations from the OMG's Model Driven Architecture (MDA) fail to satisfy one or more of these criteria, for modeling security protocols. Existing visual modeling formalisms outside the MDA also fail to satisfy one or more of these criteria. To give some examples, Petri nets, statecharts, and labeled transition systems are not event-based, compositional, or laconic; Harel's Live Sequence Charts are event-based, laconic, and compositional, but are not comprehensive.

The GSPML visual language for security protocols satisfies all of the criteria. The paper presents GSPML by example, using two security protocol models.

2.3. Authenticating With Our Minds

We present a novel idea for user authentication that we call pass-thoughts.

Recent advances in Brain-Computer Interface (BCI) technology indicate that there is potential for a new type of human-computer interaction: a user transmitting thoughts directly to a computer. The goal of a pass-thought system would be to extract as much entropy as possible from a user's brain signals upon transmitting a thought. Provided that these brain signals can be recorded and processed in an accurate and repeatable way, a pass-thought system might provide a quasi two-factor, changeable authentication method that is resistant to shoulder-surfing. The size of the space of a pass-thought system would seem to be potentially enormous, although in practice it will be finite due to system constraints and processing methods. In this talk, we discuss the motivation and potential of pass-thought authentication, and outline the design of what we believe to be a currently feasible pass-thought system.

2.4. Internet Instability and Disturbance: Goal or Menace?

Self-replicating code has become an unfortunate part of today's online environment. Viruses and worms have the ability to become pandemic within minutes of first release, and our protection systems are primarily reactive in nature. Thus, there is little or no protection from a new worm which uses a remote exploit in order to spread. Furthermore, such rapidly-moving threats have a documented ability to cause systemic outages; ultimately, such attacks may threaten the overall stability of the Internet itself. Currently, most exploits leveraged by worms have been well-known and easily solvable if the system maintainer had followed best security practices (e.g. deployed a firewall and/or carried out timely patching of vulnerabilities). Thus, actions which drive practitioners toward tighter security are likely to have a positive long-term impact on the overall stability of the global network.

In this session, we take the unusual position that low-level virus and worm outbreaks are highly beneficial to the overall goal of preventing catastrophic Internet failure. To illustrate this position we draw from a biological analogy: the Intermediate Disturbance Hypothesis. This hypothesis argues that within many natural systems it is a continual cycle of disruption which drives diversity... and hence stability and resilience. Finally, we conclude that the deliberate release of viruses and worms that are not threatening holistically may be a necessary approach to protect the Internet from catastrophic outbreaks. This position is supported by empirical evidence from the computer world and by further comparison with biological systems.