New Security Paradigms Workshop (NSPW '06)

September 19–22, 2006

Schloss Dagstuhl, Germany

The New Security Paradigms Workshop (NSPW) is a unique workshop devoted to the critical examination of new ideas in security. Each year since 1992, we have examined proposals for new principles upon which information security can be rebuilt from the ground up. Our program committee particularly looks for new paradigms: innovative approaches to older problems, early thinking on new topics, and controversial issues that might not make it into other conferences but deserve to have their try at shaking and breaking the mold.

The format of NSPW differs somewhat from other workshops. Attendance is limited to authors and workshop organizers, numbering around 30 total. All attendees are required to attend and pay attention to all presentations (no email, IM, or phone calls), without exception, so that all authors receive equal opportunity for discussion. We conduct extensive, highly interactive discussions of these proposals, from which we hope both the audience and the authors emerge with a better understanding of the strengths and weaknesses of what has been discussed. Free time outside of presentations is provided for those who have to conduct other business.

As opposed to most forums, where the authors present their papers and then answer a few questions afterward, NSPW allows questions to be asked during the presentation. As a result, although authors are given around 60 minutes for presentation, they are encour-

aged to limit their presentation material to 20 minutes and leave the rest of the time open for discussion. In some cases, authors presenting highly provocative or controversial topics may not make it past their second slide. We consider the high level of discussion to be the primary benefit of the conference, as stimulating discussion provides more feedback with which the author can refine his or her work.

Provocative work invites disagreement, especially work that is contrarian or questions the status quo. To prevent discussion from becoming an unfettered attack of the author's work, we engage the attendees in a "psychological contract," where positive feedback is strongly encouraged.

Since the discussion can provide significant feedback to the author, the final proceedings of the workshop are not published immediately at the workshop. Authors are given notes taken at their presentation, and they are expected to modify their papers based on the feedback they have received. The final proceedings are published two to three months after the workshop. The resulting papers are more complete and thought out than the original submissions.

Room and board is included in the registration fee, so that attendees can also share meals, easily participate in social activities, and not have to spend time traveling each day. This close interaction creates an atmosphere of camaraderie and provides for continued exchange of ideas.

It was my honor and pleasure this year to be the NSPW General Chair. I always find the workshop to be the most stimulating and highly enjoyable of all the workshops and conferences I attend. A terrific array of topics was presented this year, and a good time was had by all. In the following you will find a summary of the papers presented. I highly encourage researchers who have new paradigms to explore, especially risky or possibly "half-baked" ideas, to submit a paper to future New Security Paradigms Workshops.

—Abe Singer, NSPW 2006 General Chair

Sessions summarized by Matt Bishop, Michael Collins, Carrie Gates, and Abe Singer

■ *Hitting Spyware Where It Hurt$*

Richard Ford and Sarah Gordon, Florida Institute of Technology

The first paper outlined a method for retargeting click-fraud to damage spyware and adware vendors by increasing the risk associated with these methods. The authors develop a model for the return on investment for adware owners and then develop an attack aimed at disrupting the earnings of these owners by systematically sending fake requests.

The ensuing discussion focused on both the ethics and the logistics of implementing this network. An open question is the number of hosts that would be required to actually increase the risk to adware maintainers: A suggested biological analogy was the eradication of the Mexican Screw Worm in the 1970s, which was done by using sterile male Screw Worms who competed with the fertile male population. A huge number of infertile males was required to eradicate the fertile population, suggesting that an attack network would also have to be disproportionate.

■ *Dark Application Communities*

Michael Locasto, Angelos Stavrou, and Angelos Keromytis, Columbia University

This paper focused on the concept of a Dark Application Community (DAC), a botnet that forwards crash reports and other state disruptions to the bot maintainer. Essentially, the bot maintainer can acquire stack traces and other state disruptive information from normal use to acquire information on new potential vulnerabilities and threats that can then be used to generate exploitable code.

The ensuing discussion covered both the probability of successfully mining this technique for bugs and the implications for botnet management. It was pointed out that this technique extends a botnet's useful lifetime. An open question was whether this result would be more productive than fuzzing or other standard diversity techniques. Several noted the similarity between this method and n-version programming, although here the diversity is in usage rather than implementation. Possible experiments were suggested by comparing the bug discovery rates from open source auto-updated tools such as Firefox or Adium. A major concern was that, although generating reports was cheap, the cost of filtering and sorting the reports for valuable results was untenable.

■ *Challenging the Anomaly Detection Paradigm*

Carrie Gates, CA Labs; Carol Taylor, University of Idaho

This paper described weaknesses the authors perceived in the anomaly detection paradigm. The authors identified and questioned assumptions in three domains: the rarity and hostility of anomalies, problems in

training data, and incorrect assumptions about operational requirements.

In the first case, the authors argue that the assumptions made about the "normalcy" of data differ both since Denning's original studies and owing to changes in scope: Network data is more complex than system logs, and network data today is far more hostile than at the time of Denning's paper. In the second case, there are implicit assumptions about training data, such as the normalcy of a previous sample and the rarity of attacks that overlap this former case. Finally, the operational constraints were discussed in depth, with several commentators noting that the acceptable false-positive rate among the operational community is close to zero.

Inconsistency in Deception for Defense

Vicentiu Neagoe and Matt Bishop, UC Davis

This paper questions whether deceptive mechanisms, such as servers and systems that present a false view of the system, need to maintain consistent views to fool attackers. It examined the nature of inconsistency in system response and actions. The deception model divides commands into two categories: do commands (which alter system state) and tell commands (which provide information on system state). Different implementations of deception were also presented.

Discussion focused on multilevel secure systems, where commands refuse to provide status information. How do these affect the model? If the probability of deception of each occurrence of events were independent, by repeating commands an attacker could probabilistically detect deception.

A Model of Data Sanitization

Rick Crawford, Matt Bishop, Bhume Bhuiratana, Lisa Clark, and Karl Levitt, UC Davis

This paper introduced a competitive model of sanitization in the form of an inference game: a three-party game involving a sanitizer, an analyzer, and an adversary. The goal of sanitization (and the criteria for success in the game) is for the sanitizer to transform the data so that the analyst can obtain the desired information without the adversary obtaining any private information. An example was given using *k*-anonymity (e.g., a member of a set of *k* elements cannot be distinguished from any other member of the set).

Discussion focused on questions involving actively tampering with the dataset before releasing sanitized information. Examples of such attacks include salting the data beforehand and using the sanitization as a public excuse to announce something known privately (i.e., an insider requesting its own sanitized data).

Panel: Control vs. Patrol: A New Paradigm for Network Monitoring

Panelists: John McHugh, Dalhousie University; Fernando Carvalho-Rodrigues, NATO; David Townshed, University of New Brunswick

The panelists debated the idea of an independent network-monitoring authority operating to ensure network integrity. The panelists contrast their concept of patrol versus more traditional discussions of network monitoring, which, in their perspective, are control- or ownership-oriented. The analogy driving the discussion was the role of highway patrols: Where a person drives in public spaces is their own business but that they were present is publicly accessible knowledge.

The ensuing discussion focused on two elements: the logistics of such a patrol mechanism and the role and implicit privacy of users. In the former case, there were fundamental questions of what the patrol would observe and collect. Some patrol functions already exist (e.g., chatroom chaperoning), but developing a large-scale patrol involves aggregating and analyzing huge volumes of data, and deciding what classes of problems the patrol would address. Given the initial concept of privacy on the highway, there was an extensive debate about the role of privacy online, with the recognition that a user's perception of privacy is extremely contextual and possibly totally unrelated to the facts on the ground (such as blogging using a public site).

Large-Scale Collection and Sanitization of Security Data

Phil Porras, SRI; Vitaly Shmatikov, UT Austin

This paper summarized existing research challenges in data collection and sanitization for security research. Security research lacks a strong body of empirical work because of the lack of data sets; although public data sets are slowly being released, the question of sanitization is still not handled satisfactorily.

Discussion followed about how to handle the constraints of sanitization explicitly within the context of empirical research. Several suggestions focused around letting the sanitizer decide when data was released (e.g., whether some of these problems could be managed by releasing data sets after some safety period). As an alternative, a researcher may request logs of 3 consecutive days, but the sanitizer may decide which 3 consecutive days.

■ ***Googling Considered Harmful***

Greg Conti, United States Military Academy

The author began by showing AOLStalker, a search engine using the recently released (and then reclaimed) AOL dataset. This served as the context for the paper's thesis: Users increasingly rely on a large number of free services provided by a limited number of service providers. In the majority of cases, the price paid for these services is personal data: Users implicitly make micropayments of their personal privacy. The author developed a threat analysis model to privacy based on information released or gleaned from these services.

Discussion then followed on the various forms of signal analysis and social contracts previously used to protect privacy. Examples included tracking military mobilization by studying pizza deliveries in the D.C. area. Similarly noted were requirements to families of service members to keep silent before a deployment compared to the kind of logistic actions families may take en masse before a mobilization, such as communicating with various soldiers' benefits services. Discussion than focused on the construction of a privacy panel for W3C.

■ ***A Pact with the Devil***

Mike Bond, University of Cambridge; George Danezis, KU Leuven

The authors outlined a novel, and hypothetical, virus that would negotiate with its victim to improve its capacity to spread across networks. The hypothetical virus would offer an infected user a chance to commit a collaborative computer crime; for example, the original victim would write a mail that a new victim would readily open. In exchange for this, the virus would seek data on the new victim's drive (such as all of the new victim's email) and pass it on to the original victim.

Discussion focused on the strategies such a virus could take, and whether or not the victim could double-cross the virus. For example, in addition to offering carrots, the virus could eventually offer sticks such as threatening to release private or incriminating information, or planting criminal information on the victim's computer. Active comparisons were made to previous socially spreading problems (AIDS infections and the appearance of email chain letters on air-gapped networks being two prominent examples), along with consideration of what techniques would make the virus more effective, such as the scope of threats and offers the virus could make.

■ ***E-Prime for Security***

Steve Greenwald, Independent Consultant

This paper introduced E-Prime, a restricted subset of the English language developed by the General Semantics movement. E-Prime differs from English by avoiding all uses of the verb "to be," such as "is," "am," and "is not." The author argued that by eliminating these verbs, a writer is forced to provide more complete information, such as providing attribution to some action or requirement. Requiring that security policies be written in E-Prime would result in policies that are easier to read and that do not include assumed information. For example, "The administrator is required to provide audit logs" would become "The security team requires the administrator to provide audit logs."

■ ***Diffusion and Graph-Spectral Methods for Network Forensic Analysis***

Wei Wang and Tom Daniels, Iowa State University

This paper described a graph-theoretic approach to analyzing audit logs and network traffic with the aim of detecting attacks. The approach used was to have each node represent a host, for example, while connections between nodes would represent events. These events would have a weight associated with them that was based on some quality of the event or alert. The authors used eigenvectors to determine qualities of the network, finding that the first three eigenvectors often did not result in interesting information; however, the fourth eigenvector could isolate attacks.

The authors used data from the Lincoln Labs data set for testing, and so discussion focused on how this approach would perform given data from a real network. The primary issue discussed was what effect the noise inherent in a real network would have on the ability for this approach to extract attack information.

■ ***PKI Design for the Real World***

Peter Gutmann, U. Auckland; Ben Laurie, Google; Bob Blakley, Burton Group; Mary-Ellen Zurko, IBM; Matt Bishop, UC Davis

Each panelist described his or her belief about PKI and its adoption in the real world. Zurko started, describing the PKI system currently in use by Lotus Notes at IBM. This is a system that is deployed at many large enterprises and has been in use for several years. Laurie felt that the issue with PKI was the I: The infrastructure required for PKI was lacking. In particular, he noted that there were two requirements that needed to be met: (1) You want to know that

the person you are talking to today is the same person you were talking to yesterday, and (2) you want to know that the person you are talking to is the same person you were introduced to. Blakley, in contrast, felt that PKI was developed for two reasons: (1) Key distribution is hard and should be easier, and (2) digital signatures are cool. As a result, he felt that the main problem with PKI was that it was designed to solve a problem that no one had, and that PKI does not mimic any real-world processes. Bishop felt that the issue with PKI was that the design of the system is not understandable. For example, many nontechnical users do not understand what a chain of trust is. This also introduced legal issues, such as who has root and what does it mean to trust them? He felt that PKI was workable on a personal level (e.g., PGP) and at the level of a corporation, but not among the general public. Gutmann focused on a study he performed asking senior engineers and managers how they would design a PKI system given the constraint that they would need to support their design. He found that the systems described were all Web-based and differed completely from the designs proposed in the standards committee.