Announcement and Preliminary Call for Papers

1st USENIX Workshop on Intrusion Detection and Network Monitoring

For more information about this workshop, see http://www.usenix.org/events/detection99

April 11-12, 1999
Santa Clara Marriott Hotel
Santa Clara, California

This Call for Papers is preliminary. Deadlines and instructions may undergo minor changes. Authors should check ***http://www.usenix.org/events/detection99/cfp.html*** for final instructions after October 15, 1998.

Important Due Dates for Refereed Paper Submissions

Extended abstracts due: *November 1, 1998*
Notification to authors: *November 23, 1998*
Full papers for editorial review: *December 12, 1998*
Camera-ready full papers: *February 23, 1999*

Program Committee

Chair: Marcus J. Ranum, *Network Flight Recorder*
Charles Antonelli, *University of Michigan*
Frederick Avolio, *Avolio Consulting*
Tina Darmohray, *System Experts*
Rik Farrow, *Consultant*
Dan Geer, *CERTCO*
Norm Laudermilch, *UUNet/Worldcom*

Overview

The goal of this workshop is to bring together network managers, engineers and researchers interested in deploying and developing intrusion detection systems (IDS) and network monitoring technologies for security, traffic analysis, or forensics. The workshop will emphasize practical results, case studies, and real-world large-scale deployment of ID.

This will be a two-day workshop, consisting of invited talks, refereed papers, and work-in-progress reports. Opportunities to get together informally will include a Sunday evening hosted reception, a hosted lunch on Monday with Marcus Ranum chairing, and Birds-of-a-Feather sessions on Sunday.

Technical Sessions

Intrusion detection offers the promise of automatic detection and notification of break-ins or unauthorized use of computers. With networks becoming increasingly interconnected, it`s difficult to draw a clear boundary between "internal" and "external" — better techniques for detecting abuse from within are becoming mandatory.

We seek papers describing original work concerning the design, implementation, and real-world application of intrusion detection and network monitoring technologies. Besides mature work, we encourage submissions describing exceptionally promising prototypes, or enlightening negative results. Case studies and experience papers are particularly of interest. Share your results, share your pain, share your ideas.

Where appropriate, authors will be able to demonstrate their applications during their presentation using systems that will be fed with packets captured at "live" sites, which contain various intrusion attempts. Also, space will be available to authors to demonstrate their work outside of their presentation in a more relaxed and interactive environment.

Topics

Topics of interest include, but are not limited to:

Case studies of IDS in practice
Statistical models for IDS
Anomaly detection systems
Misuse detection systems
Host based approaches to IDS
Network based approaches to IDS
Application-based approaches to IDS
IDS in cryptographically protected networks
Distributed IDS in large networks
Correlation techniques
Event thresholding
Reducing false positives
Alternative approaches

What To Submit

Authors must submit an extended abstract by Nov 1, 1998. This should be 5-7 pages long or about 2500-3500 words, not counting references and figures. You may submit a full paper for use by the program committee if there are questions about the abstract, but the full paper is not required. Longer submissions, not accompanied by an appropriate extended abstract, will be penalized in the review process.

The full papers resulting from accepted abstracts will go through an editorial review cycle with a member of the program committee, and should end up about 10-12 pages long.

The objective of an extended abstract is to convince the reviewers that a good paper and 25-minute presentation will

result. It is important to identify what has been accomplished, to explain why it is significant, and to compare with prior work in the field, demonstrating knowledge of the relevant literature. The extended abstract should represent the paper in "short form." It must include the abstract as it will appear in the final paper. The body of the extended abstract should be complete paragraphs, not just an outline of the paper. (Sections present in the full paper but omitted from the abstract may be summarized in terse form.) Authors should include full references, figures when available, and as is usually appropriate, performance data. Such data also help indicate the status of the implementation, often a crucial issue. The abstract will be judged on significance, originality, clarity, relevance, and correctness.

This Workshop, like most conferences and journals, requires that papers not be submitted simultaneously to another conference or publication and that submitted papers not be previously or subsequently published elsewhere. All submissions will be held in the strictest confidence prior to publication. Papers accompanied by so called "non-disclosure agreement" forms are not acceptable and will be returned unread.

Please read the detailed author guidelines. For a copy of the author guidelines, either see **http://www.usenix.org/events/detection99/guidelines.html**, or send email to **detection99authors@usenix.org**.

How To Submit

The current Call for Papers is preliminary. Deadlines and instructions may undergo minor changes. Authors should check the USENIX Association Web page (www.usenix.org) for final instructions after October 15.

Submissions should be done electronically via email. Make submissions to **detection99papers@usenix.org**.

A form will be provided on the Web to facilitate submission and ensure that all submissions provide all the information that is required. This information will include:

1. The title of the paper and the names and affiliations of all authors. (Note: authors' names and affiliations will be known to the reviewers).
2. The name, email and postal addresses, day and evening phone numbers, and a fax number if available, of one author who will serve as a contact.
3. An indication of which, if any, of the authors are full-time students.

The alternate method of submission will remain postal mail; you may mail 15 copies of your submission to:

Marcus J. Ranum
16400 Ed Warfield Rd
Woodbine, MD 21797
410-489-4995

All submissions will be acknowledged electronically; you must provide an email address. If you have not received an acknowledgment within 60 hours of submitting your abstract electronically (or the submission deadline, if the submission is early), please contact the program chair at **detection99chair@usenix.org**.

Work-In-Progress Reports

Do you have interesting work you would like to share, or a cool idea that is not ready to be published? Works-in-progress reports are for you! Works-in-progress reports, scheduled during the technical sessions, introduce new or ongoing work. The USENIX audience provides valuable discussion and feedback. We are particularly interested in presentations of student work. To schedule your report, please contact the Works-in-Progress coordinator at **detection99wips@usenix.org**.

Program/Registration Materials

Materials containing all details of the technical program, registration fees and forms, and hotel information will be available online at **http://www.usenix.org/events/detection99/** and in print in January 1999. If you wish to receive the printed program materials, please contact:

USENIX Conference Office
22672 Lambert Street, Suite 613
Lake Forest, CA 92630 USA
Phone: +1 949-588-8649
Fax: +1 949-588-9706
Email: **conference@usenix.org**