REGISTER EARLY AND SAVE!

15th Annual Network and Distributed System Security Symposium

The Dana on Mission Bay • San Diego, California
February 10-13, 2008

Learn From Leading Network Security Researchers and Practitioners

Who Attends

- ✓ University Researchers and Educators
- ✓ Chief Technology and Privacy Officers
- ✓ Security Analysts and System Administrators
- ✓ Operations and Security Managers

PATRON SPONSOR

SILVER SPONSORS

Afilias
GLOBAL REGISTRY SERVICES

Google

SDSC
SAN DIEGO SUPERCOMPUTER CENTER

BRONZE SPONSORS

Microsoft Research

Dartmouth College
INSTITUTE FOR SECURITY TECHNOLOGY STUDIES

IEEE MEDIA SPONSOR

IEEE SECURITY & PRIVACY

SUPPORTED BY

Internet Society

NDSS '08 Steering Group

Douglas Szajda, University of Richmond
Crispin Cowan, Mercenary Linux
Giovanni Vigna, University of California, Santa Barbara
Tom Hutton, San Diego Supercomputer Center
Barry Lawson, University of Richmond
William Arbaugh, University of Maryland
Eric Harder, National Security Agency
Angelos Keromytis, Columbia University
Fabian Monrose, Johns Hopkins University
Michael Roe, Microsoft, UK
Karen Seo, BBN Technologies
Dan Simon, Microsoft Technologies
Dawn Song, University of California, Berkeley
David Wagner, University of California, Berkeley
Pieter "Mudge" Zatko, BBN Technologies

NDSS '08 Program Committee

Crispin Cowan, Mercenary Linux
Giovanni Vigna, UC Santa Barbara
Lujo Bauer, Carnegie Mellon University
Konstantin Beznosov, University of British Columbia
John Black, University of Colorado
David Brumley, Carnegie Mellon University
Jon Callas, PGP
Hao Chen, UC Davis
Charles Clarke, University of Waterloo
Vinod Ganapathy, University of Wisconsin
Jonathon Giffin, Georgia Institute of Technology
Farnam Jahanian, University of Michigan
Angelos Keromytis, Columbia University
Engin Kirda, Vienna University of Technology
Christopher Kruegel, Vienna University of Technology
Ben Laurie, Google
Wenke Lee, Georgia Institute of Technology
Michael Locasto, Columbia University
Fabian Monrose, Johns Hopkins University
Niels Provos, Google
Len Sassaman, Katholieke Universiteit Leuven
R. Sekar, SUNY Stonybrook
Sean Smith, Dartmouth College
Zhendong Su, UC Davis
Nick Weaver, ICSI

15th Annual Network and Distributed System Security Symposium
The Dana on Mission Bay
San Diego, California • February 10-13, 2008

Learn from leading network security researchers and practitioners

Register today for the Network and Distributed System Security Symposium, NDSS '08. Now in its 15th year, the NDSS Symposium is recognized as one of the leading annual events for information exchange among researchers and practitioners of network and distributed system security services. This information-packed event covers the latest in network security, with paper presentations and panel discussions by leading experts.

Featuring new research with practical applications

NDSS '08 will focus on practical aspects of network and distributed system security, with emphasis on actual system design and implementation rather than theory. A major goal of the Symposium is to encourage and enable the Internet community to apply, deploy, and advance the state of available security technology. Summaries of papers to be presented can be found on the following pages.

Keynote presentation by Gary McGraw

Gary McGraw is the CTO of Cigital, Inc., a software security and quality consulting firm with headquarters in the Washington, D.C. area. He is a globally recognized authority on software security and the author of six best selling books on this topic. The latest, *Exploiting Online Games* was released in 2007. His other titles include *Java Security, Building Secure Software, Exploiting Software,* and *Software Security;* and he is editor of the Addison-Wesley Software Security series.

Symposium Schedule

Sunday, February 10

4:30 pm - 7:30 pm	Registration
6:00 pm - 8:00 pm	Welcome Reception

Monday, February 11

7:30 am	Continental Breakfast
8:30 am - 10:30 am	Opening & Keynote: Breaking Online Games Gary McGraw, Cigital, Inc.
11:00 am - 12:30 pm	Technical Presentations
12:30 pm - 1:30 pm	Lunch
1:30 pm - 5:00 pm	Technical Presentations
6:30 pm - 9:30 pm	Dinner

Tuesday, February 12

7:30 am	Continental Breakfast
8:30 am - 12:00 noon	Technical Presentations
12:00 noon - 1:30 pm	Lunch
1:30 pm - 3:00 pm	Virtualization & Security Panel
3:30 pm - 5:00 pm	Technical Presentations
6:30 pm - 9:30 pm	Dinner

Wednesday, February 13

8:00 am	Continental Breakfast
9:00 am - 10:30 am	Invited Talk: "Breaking Stuff" Dan Kaminsky, Dox Para Research*
11:00 am - 12:30 pm	Technical Presentations
12:30 pm -1:30 pm	Lunch
1:30 pm - 3:00 pm	Gong Show
3:00 pm - 3:30 pm	Closing Remarks

**Invited, not confirmed*

Visit the NDSS '08 website for more details: www.isoc.org/ndss08

15th Annual Network and Distributed System Security Symposium
Paper Presentations

Exploiting Opportunistic Scheduling In Cellular Data Networks

Radmilo Racic, Hao Chen, *and* **Xin Liu,** *University of California, Davis;* **Denys Ma,** *McAfee*

Rogue cellular devices within a 3G network relying on opportunistic scheduling algorithms, namely Proportional Fair (PF) and its variants, can exploit PF's as well 3G's vulnerabilities allowing them to usurp the majority of all time slots. Our simulations show that only one rogue device per cell that has 50 users can use up to 90% of the time slots, and can cause a 1.11-second end-to-end inter-packet transmission delay on VoIP applications of every other user in the same cell, effectively rendering the VoIP service useless. To defend against the attacks, we explore a set of attack detection schemes, discuss a variety of modifications to the PF scheduler and their resilience to the attacks, and propose a novel robust handoff algorithm that manages to mitigate the aforementioned attacks.

A Tune-up for Tor: Improving Security and Performance in the Tor Network

Robin Snader, *and* **Nikita Borisov,** *University of Illinois at Urbana-Champaign*

The Tor anonymous communication network uses self-reported bandwidth values to select routers for building tunnels. Since tunnels are allocated in proportion to this bandwidth, this allows a malicious router operator to attract tunnels for compromise. We propose an opportunistic bandwidth measurement algorithm to replace self-reported values and address both of these problems. We also propose a mechanism to let users tune Tor performance to achieve higher performance or higher anonymity. Our mechanism effectively blends the traffic from users of different preferences, making partitioning attacks difficult.

HookFinder: Identifying and Understanding Malware Hooking Behaviors

Heng Yin, *and* **Zhenkai Liang,** *Carnegie Mellon;* **Dawn Song,** *UC Berkeley*

Installing various hooks into the victim system is an important attacking strategy used by malware, including spyware, rootkits, stealth backdoors, and others. In this paper, we propose the first systematic approach to automatically identifying hooks and extracting the hook implanting mechanisms. We propose fine-grained impact analysis, as a unified approach to identify hooking behaviors of malicious code. We have developed a prototype, HookFinder, and conducted extensive experiments using representative malware samples from various categories.

Would Diversity Really Increase the Robustness of the Routing Infrastructure against Software Defects?

Juan Caballero, *and* **Theocharis Kampouris,** *Carnegie Mellon University;* **Dawn Song,** *Carnegie Mellon University and UC Berkeley;* **Jia Wang,** *AT&T Labs-Research*

Network diversity has been proposed as a solution to increase the resilience to software defects, but the benefits have not been clearly studied. In this paper, we find that a small degree of diversity in the network can provide good robustness against simultaneous router failures. In particular, for a large Tier-1 ISP network, five implementations suffice. We observe that the best way of applying diversity is to partition the network into contiguous regions that use the same implementation, taking into account the node roles and possibly replicated nodes.

Automated Whitebox Fuzz Testing

Patrice Godefroid, *Microsoft Research;* **Michael Y. Levin,** *Microsoft Center for Software Excellence; and* **David Molnar,** *UC Berkeley & Microsoft*

We present an alternative whitebox fuzz testing approach inspired by recent advances in symbolic execution and dynamic test generation. Our approach records an actual run of a program under test on a well-formed input, symbolically evaluates the recorded trace, and generates constraints capturing how the program uses its inputs. We have implemented this algorithm in SAGE (Scalable, Automated, Guided Execution), a new tool employing x86 instruction-level tracing and emulation for whitebox fuzzing of arbitrary file-reading Windows applications. We describe key optimizations needed to make dynamic test generation scale to large input files and long execution traces with hundreds of millions of instructions. While still in an early stage of development, SAGE has already discovered 30+ new bugs in large shipped Windows applications including image processors, media players, and file decoders.

Automatic Protocol Format Reverse Engineering through Context-Aware Monitored Execution

Zhiqiang Lin, Dongyan Xu *and* **Xiangyu Zhang,** *Purdue University;* **Xuxian Jiang,** *George Mason University*

In this paper, we present a system named AutoFormat that aims at not only extracting the protocol fields with high accuracy, but also revealing the inherent "non-flat" hierarchical structures of protocol messages. AutoFormat is based on the key observation that different protocol fields in the same message are typically handled in different execution contexts (e.g., the run-time call stack). As such, by monitoring the program's execution, we can collect such execution context information for every message byte (annotated with its offset in the entire message), and then cluster the collected information to derive the protocol format.

Corrupted DNS Resolution Paths: The Rise of a Malicious Resolution Authority

David Dagon, Chris Lee *and* **Wenke Lee,** *Georgia Institute of Technology;* **Niels Provos,** *Google Inc.*

We study and document an important development in how attackers are using Internet resources: the creation of malicious DNS resolution paths. In this growing form of attack, victims are forced to use rogue DNS servers for all resolution. To document the rise of this "second secret authority" on the Internet, we studied instances of aberrant DNS resolution on a university campus. We found dozens of viruses that corrupt resolution paths, and noted that hundreds of URLs discovered per week performed drive-by alterations of host DNS settings.

Taming the Devil: Techniques for Evaluating Anonymized Network Data

Scott Coull, Charles Wright *and* **Fabian Monrose,** *Johns Hopkins University;* **Angelos Keromytis,** *Columbia University;* **Michael Reiter,** *University of North Carolina*

Anonymization plays a key role in enabling the public release of network datasets, yet there are few, if any, techniques for evaluating the efficacy of network data anonymization techniques with respect to the privacy they afford. Specifically, we simulate the behavior of an adversary whose goal is to deanonymize objects, such as hosts or web pages, within the network data. By doing so, we are able to quantify the anonymity of the data using information theoretic metrics, objectively compare the efficacy of anonymization techniques, and examine the impact of selective deanonymization on the anonymity of the data.

Realizing Massive-Scale Conditional Access Systems Through Attribute-Based Cryptosystems

Patrick Traynor, Kevin Butler, William Enck, *and* **Patrick McDaniel,** *Penn State University*

In this paper, we explore the ability of attribute-based encryption (ABE) to meet the unique performance and security requirements of conditional access systems such as subscription radio and pay-per-view television. We show through empirical study that costs of ABE make its direct application inappropriate, but present constructions that mitigate its incumbent costs. We develop an extensive simulation that allows us to explore the performance of a number of virtual hardware

configurations and construction parameters over workloads developed from real subscription and television audiences.

Analyzing Privacy in Enterprise Packet Trace Anonymization

Bruno Ribeiro, Gerome Miklau *and* **Don Towsley,** *UMass Amherst;* **Weifeng Chen,** *John Jay College of Criminal Justice*

In this work we present a novel, systematic attack on prefix-preserving anonymization which can be efficiently executed by an adversary in possession of a modest amount of public information about the network. The attack is general (encompassing a range of fingerprinting attacks proposed by others) and flexible (it can be adapted to emerging variants of prefix-preserving anonymization). Perhaps most importantly, we develop analysis tools that allow data publishers to quantify the worst-case vulnerability of their trace given assumptions about the adversary's external information. Using this analysis we quantify the trade-off between privacy and utility of alternatives to full prefix-preserving anonymization.

Halo—High Assurance Locate for Distributed Hash Tables

Apu Kapadia, *Dartmouth College; and* **Nikos Triandopoulos,** *University of Aarhus, Denmark*

We study the problem of reliably searching for resources in untrusted peer-to-peer networks, where a significant portion of the participating network nodes act maliciously. We present a new method called Halo for performing redundant searches over a distributed hash table (DHT) structure that achieves high integrity levels without affecting the storage and communication complexities of the underlying DHT. In particular, a querier can successfully locate the network node storing an object despite the presence of malicious nodes trying to subvert the locate operation.

Robust Receipt-Free Election System with Ballot Secrecy and Verifiability

Sherman S.M. Chow, *New York University;* **Joseph K. Liu,** *Institute for Infocomm Research, Singapore; and* **Duncan S. Wong,** *City University of Hong Kong*

We propose a new way of constructing vote-and-go election system without tamper-resistant hardware, randomizer, or anonymous channel. Receipt-freeness is guaranteed even if there is only one voting authority (in a distributed setting) remains honest. Regarding the correctness, voter alone has no chance to tamper with the validity of the final tally, while any misbehaving authority can be detected (and proven to the public) by the tallying center. Robustness can be achieved by fixing the corrupted vote in a verifiable manner. Ballot secrecy cannot be compromised even if all tallying authorities collude.

Analysis-Resistant Malware

John Bethencourt, Dawn Song, *University of California, Berkeley / Carnegie Mellon University; and* **Brent Waters,** *SRI International*

Traditionally, techniques for computing on encrypted data have been proposed with privacy preserving applications in mind. Several current cryptosystems support a homomorphic operation, allowing simple computations to be performed using encrypted values. This is sufficient to realize several useful applications, including schemes for electronic voting and single server private information retrieval (PIR). In this paper, we introduce an alternative application for these techniques in an unexpected setting: malware. We point out the possibility of malware which renders some aspects of its behavior provably resistant to forensic analysis, even with full control over the malware code, its input, and its execution environment.

Limits of Learning-based Signature Generation with Adversaries

Shobha Venkataraman, Avrim Blum, *and* **Dawn Song,** *Carnegie Mellon University*

In this paper, we show fundamental limits on the accuracy of pattern-extraction algorithms for signature-generation in an adversarial setting. We formulate a natural framework that allows a unified analysis of these algorithms, and prove lower bounds on the number of mistakes any pattern-extraction learning algorithm must make under common assumptions, by showing how to adapt results from learning theory. While previous work has targeted specific algorithms, the work of these three authors generalizes these attacks through theoretical analysis to any algorithm with similar assumptions, not just the techniques developed so far.

Usable PIR

Peter Williams, *and* **Radu Sion,** *Stony Brook University*

In "On the Practicality of Private Information Retrieval" (NDSS '07) we showed that existing single-server computational private information retrieval (PIR) protocols for the purpose of preserving client access patterns leakage are orders of magnitude slower than trivially transferring the entire data sets to the inquiring clients. We thus raised the issue of designing efficient PIR mechanisms in practical settings. In this paper we introduce exactly such a technique, guaranteeing access pattern privacy against a computationally bounded adversary, in outsourced data storage, with communication and computation overheads orders of magnitude better than existing approaches. In the presence of a small amount (O(sqrt n), where n is the size of the database) of temporary storage, clients can achieve access pattern privacy with communication and computational complexities of less than O(log^2 n) per query (as compared to e.g., O(log^4 n) for existing approaches). We achieve these novel results by applying new insights based on probabilistic analyses of data shuffling algorithms to Oblivious RAM, allowing us to significantly improve its asymptotic complexity.

Automatic Network Protocol Analysis

Gilbert Wondracek, Christopher Kruegel *and* **Engin Kirda,** *Technical University Vienna;* **Paolo Milani,** *Scuola Superiore S. Anna, Italy*

In this paper, we present a novel approach to automatic protocol reverse engineering. The approach works by dynamically monitoring the execution of the application, analyzing how the program is processing the protocol messages that it receives. This is motivated by the insight that an application encodes the complete protocol and represents the authoritative specification of the inputs that it can accept. In a first step, the authors extract information about the fields of individual messages. Then, they aggregate this information to determine a more general specification of the message format, which can include optional or alternative fields.

A New Privacy-Enhanced Matchmaking Protocol

Ji Sun Shin *and* **Virgil D. Gligor,** *University of Maryland*

Although several wide-spread Internet applications (e.g., job-referral services, dating services) can benefit from online matchmaking, protocols defined over the past two decades fail to address important privacy concerns. In this paper, we enhance traditional privacy requirements (e.g., user anonymity, matching-wish authenticity) with new privacy goals (e.g., resistance to off-line dictionary attacks, and forward privacy of users' identities and matching wishes), and argue that privacy-enhanced matchmaking cannot be provided by solutions to seemingly related problems such as secret handshakes, set intersection, and trust negotiation. We define an adversary model, which captures the key security properties of privacy-enhanced matchmaking, and show that a simple, practical protocol derived by a two-step transformation of a password-based authenticated key exchange counters adversary attacks in a provable manner.

BotSniffer: Detecting Botnet Command and Control Channels in Network Traffic

Guofei Gu, Junjie Zhang, *and* **Wenke Lee,** *Georgia Institute of Technology*

Botnets are now recognized as one of the most serious threats to Internet security. In contrast to previous malware, botnets have the characteristic of a command and control (C&C) channel. Botnets also often use existing common protocols, e.g., IRC, HTTP (and in protocol-conforming manners), making the detection of botnet C&C activities a challenging problem. In this paper, we propose using network-based anomaly detection to identify botnet C&C channels in a local network without any prior knowledge of signatures or C&C server addresses. This detection approach can help identify both the C&C servers and infected hosts in the network.

Impeding Malware Analysis using Conditional Code Obfuscation

Monirul Sharif, Jonathon Giffin *and* **Wenke Lee,** *Georgia Institute of Technology;* **Andrea Lanzi,** *Universita` degli Studi di Milano, Italy*

In this paper, we present a malware obfuscation technique that automatically conceals specific condition dependent malicious behavior from malware analyzers that have no prior knowledge of program inputs. Our technique, which is well-suited for concealing trigger-based behavior, automatically transforms a program by encrypting code that is conditionally dependent on some input value with a key derived from the input and then removing the key from the program. We have implemented a compiler-level tool that takes a malware source program and automatically generates an obfuscated binary. Experiments on various existing malware samples show that our tool can hide a significant portion of trigger based code.

PRECIP: Practical and Retrofittable Confidential Information Protection Against Spyware Surveillance

XiaoFeng Wang, Zhuowei Li, *School of Informatics, Indiana University;* **Ninghui Li,** *Purdue University; and* **Jong Youl Choi,** *School of Informatics, Indiana University*

A grand challenge in information protection is how to preserve the confidentiality of sensitive information under spyware surveillance. This problem has not been well addressed by the existing access-control mechanisms which cannot prevent the spyware already in a system from monitoring an authorized party's interactions with sensitive data. Our answer to this challenge is PRECIP, a new security policy model for practical and retrofittable confidential information protection. This model is designed to offer efficient online protection for commercial applications and operating systems. It intends to be retrofitted to these applications and systems without modifying their code.

Detection and Mitigation of Fast-Flux Service Networks

Thorsten Holz, Christian Gorecki, Felix Freiling, *University Mannheim, Germany; and* **Konrad Rieck,** *Fraunhofer FIRST, Germany*

We present the first empirical study of fast-flux service networks (FFSNs), a newly emerging and still not widely-known phenomenon in the Internet. FFSNs employ DNS to establish a proxy network on compromised machines through which illegal online services can be hosted with very high availability. Through our measurements we show that the threat which FFSNs pose is significant: FFSNs occur on a worldwide scale and already host a substantial percentage of online scams. Based on analysis of the principles of FFSNs, we develop a metric with which FFSNs can be effectively detected. Based on our detection technique we also discuss possible mitigation strategies.

Symposium Venue

The Dana on Mission Bay will serve as the host hotel for NDSS '08. Surrounded by 10 acres of tropical landscape and connected to 27 miles of waterfront paths, the Dana is the closest hotel to San Diego's famous SeaWorld. A limited block of rooms has been set aside for NDSS '08 participants. *Make your reservations early to avoid disappointment. Single and Double rooms are available at $159 plus tax.*

Make your reservations by calling the Dana directly at 1.800.445.3339 or 1.619.222.6440 and requesting the group rate for the "NDSS Symposium." To book online at the Dana website (www.thedana.com), click "Reservations" then on "Group Reservations." Then enter the Attendee Code "NDSSGROUP" and login to make your reservations at the group rate.

The Dana on Mission Bay
1710 West Mission Bay Drive
San Diego, CA 92109-7899
www.thedana.com
US: 800.445.3339
Outside the US: +1 619.222.6440

Reservations cut-off date: January 11, 2008
Check-in time is 4:00 pm.
Check-out time is 12:00 noon.

Airport Transfers

The Dana on Mission Bay operates a complimentary shuttle for guests arriving at San Diego International Airport. The shuttle service is available from 7 am to 10 pm by calling the hotel at 619.222.6440 upon arrival at the airport. The shuttle is also available to transport guests to nearby Sea World according to a predetermined daily schedule available at the hotel's front desk.

N D S S '08 SYMPOSIUM

REGISTRATION FORM

15th Annual Network and Distributed System Security Symposium

The Dana on Mission Bay • San Diego, California
February 10-13, 2008

PERSONAL INFORMATION

FIRST NAME _____ LAST NAME _____

JOB TITLE _____

COMPANY, ORGANIZATION, AGENCY OR INSTITUITON _____

ADDRESS _____

CITY _____ STATE/PROVINCE _____ ZIP/POSTAL CODE _____ COUNTRY _____

PHONE _____ FAX _____ E-MAIL _____

REGISTRATION FEE (please check the appropriate box)

	By Dec 21	Dec 22 - Jan 25	After Jan 25
Symposium Participant	☐ $720	☐ $850	☐ $970
Symposium Speaker	☐ $720	☐ $720	☐ $720
Full-Time Student*	☐ $295	☐ $310	☐ $325

*Student registration fee available only upon verification of student status. Please send documentation showing that you are a full-time student *(copy of transcript or letter from your department)* by fax or mail to the Internet Society address below.

PAYMENT METHOD: Pay by check, MasterCard, Visa or American Express. Please provide all the information requested below.

☐ Check (drawn on US bank account) ☐ Master Card ☐ Visa ☐ American Express

CREDIT CARD NUMBER _____ EXPIRATION DATE ____/____/____

CARDHOLDER NAME _____

CARDHOLDER SIGNATURE _____

Check this box if you have a disability which requires special accommodation. ☐
Check the appropriate box if you have any special dietary requirements:

☐ *Kosher* ☐ *Vegetarian* ☐ *Other:* _____

Multiple Registration Discount: When two or more Symposium Participants from the same organization register at the same time, each registration may be discounted by $100. To be eligible for this discount, you must mail or fax all registrations and payments from your organization together or, if registering the individuals online, notify us with an email that includes the names of all of the registrants from your organization. This email should be sent to: ndss08reg@isoc.org. *The Multiple Registration Discount does not apply to Student registrations.*

Social Passes: Social Passes are available for guests who accompany registrants to the Symposium. Social Passes provide admission to meal and social functions, but not Symposium sessions. Symposium registrants may purchase Social Passes, in advance, for up to 3 guests at US $150 each.

Wire Transfers: Persons unable to pay registration fees by credit card or check may pay by wire transfer. Please process wire transfers before sending your registration form. Include your full name and the letters "NDSS" with wire transfer. Please contact **ndss08reg@isoc.org** for detailed wire transfer instructions.

Terms & Conditions: Symposium registration includes admission to all Symposium sessions, Proceedings book and CD, and specified meals and refreshment breaks. Travel and lodging arrangements and other expenses are the sole responsibility of participants. Program content and speakers are subject to change without notice. Contact information you provide will be published in the Symposium participant roster provided to registered participants.

Registration Cancellation Policy: 90% of the registration fee will be refunded for cancellations received in writing on or before 31st December 2007. No refunds will be issued after 31st December 2007; however, a substitute participant will be accepted at any time with advance written notification. For information concerning the hotel's reservation cancellation policy and procedures, contact the Dana on Mission Bay.

Four easy ways to register

1. **Mail:** Internet Society
   1775 Wiehle Avenue, Suite 102
   Reston, VA 20190 U.S.A.
2. **Fax:** 1.703.326.9881
3. **E-mail:** ndss08reg@isoc.org
4. **Internet:** www.isoc.org/ndss08

N D S S '08
SYMPOSIUM

Internet Society
1775 Wiehle Avenue, Suite 102
Reston, Virginia 20190-5108 USA

15th Annual Network and Distributed System Security Symposium

The Dana on Mission Bay
San Diego, California
February 10-13, 2008

Internet Society

REGISTER EARLY AND SAVE!

Registration includes admission to all symposium sessions, proceedings book, CD, meals, and refreshment breaks throughout the event.

Learn From Leading Network Security Researchers and Practitioners