Recent Advances in Intrusion Detection 2006
September 20-22, 2006
University of Hamburg "Edmund Siemers Allee 1," Hamburg, Germany
Register at: http://www.raid06.tu-harburg.de/registration.html

Call for Participation and Poster Proposals
This symposium, the ninth in an annual series, brings together leading researchers and practitioners from academia, government, and industry to discuss issues and technologies related to intrusion detection and defense. The Recent Advances in Intrusion Detection (RAID) International Symposium series is intended to further advances in intrusion defense by promoting the exchange of ideas in a broad range of topics.

This year, the RAID program includes sixteen full presentations selected from almost 100 submissions, with proceedings published by Springer. The program also includes invited speakers and a poster session. RAID will accept poster submissions until August 6th.
The RAID organizing committee calls for the participation of the global IT security professional and research communities.

Preliminary Program
Wednesday, September 20th, 2006: Registration starts at 9:00
12:30–14:00 Lunch
14:00–14:15 Welcome to RAID 2006
14:15–15:15 Invited Talk
15:45–16:45 Session: Anomaly Detection
16:45–17:30 Session: Intrusion Detection with Integrated Sampling and Learning
17:30–18:00 Poster abstract session (5-minute talks)
18:00–20:00 Poster session
Thursday, September 21st, 2006
09:00–10:30 Session: Attacks
Automated Discovery of Mimicry Attacks
Jonathon T. Giffin, Somesh Jha, and Barton P. Miller
Allergy Attack Against Automatic Signature Generation
Simon P. Chung and Aloysius K. Mok
Paragraph: Thwarting Signature Learning By Training Maliciously
James Newsome, Brad Karp, and Dawn Song
11:00–12:30 Session: System Evaluation and Threat Assessment
Anomaly Detector Performance Evaluation Using A Parameterized Environment
Jeffery P. Hansen, Kymie M.C. Tan and Roy A. Maxion
Ranking Attack Graphs
Vaibhav Mehta, Constantinos Bartzis, Hai Feng Zhu, Edmund Clarke, and Jeanette Wing
Using Hidden Markov Models to Evaluate The Risks Of Intrusions–System Architecture And Model Validation
Andre Arnes, Fredrik Valeur, Giovanni Vigna, and Richard A. Kemmerer
12:30–14:00 Lunch
14:00–15:00 Invited Talk
15:30–17:00 Session: Malware Collection and Analysis
The Nepenthes Platform: An Efficient Approach To Collect Malware
Paul Baecher, Markus Koetter, Thorsten Holz, Maximillian Dornseif, and Felix Freiling
Automatic Handling of Protocol Dependencies & Reaction To 0-Day Attacks With ScriptGen-Based Honeypots
Corrado Leita, Marc Dacier, and Frederic Massicotte
Fast and Evasive Attacks: Highlighting The Challenges Ahead
Mohede Abu Rajab, Fabian Monrose, and Andreas Terzis
Friday, September 22nd, 2006
09:00–10:00 Session: Anomaly- and Specification-Based Detection
Anagram: A Content Anomaly Detector Resistant to Mimicry Attack
Ke Wang, Janak J. Parekh, and Salvatore J. Stolfo
DEMEM: Distributed Evidence-Driven Message Exchange Intrusion Detection Model for MANET
Chinyang Henry Tseng, Shiu-Huey Wang, Calvin Ko, and Karl Levitt
10:30–12:00 Session: Network Intrusion Detection
Enhancing Network Intrusion Detection with Integrated Sampling and Filtering
Jose M. Gonzalez and Vern Paxson
WIND: Workload-Aware Intrusion Detection
Sushant Sinha, Farnam Jahanian, and Jignesh M. Patel
12:00–12:15 Concluding remarks

Organizing Committee
General Chairs: Dieter Gollmann (Technical University Hamburg-Harburg, diego@gollmann-harburg.de), Andreas Frauenhi-Jstech)
Program Chair: Diego Zamboni (IBM Zurich Research Laboratory, dza@zurich.ibm.com)
Publication Chair: James Riordan (IBM Zurich Research Laboratory, rjord@zurich.ibm.com)
Publicity Chair: Robert Cunningham (MIT Lincoln Laboratory, rke@ll.mit.edu)
Sponsorship Chair: Klaus-Peter Kossakovski (PRESECURE Consulting, kpk@gse-security.de)

Steering Committee
Chair: Marc Dacier (Eurowecom, France)
Herve Debar (France Telecom R&D, France)
Deborah Frincke (Pacific Northwest National Lab, USA)
Ming-Yah Huang (The Boeing Company, USA)
Erland Jonsson (Chalmers, Sweden)
Kwok-Tung Wong (Chinese University of Hong Kong, China)
Kees van Reeuwijk (TNO, The Netherlands)
Wolfgang Nejdl (Max-Planck Institute for Informatics, Germany)
Kees van der Schaft (IBM Zurich Research Laboratory, kvs@zurich.ibm.com)
Kris Yokoyama (IBM Tokyo Research Laboratory, kyoko@ibm.co.jp)

Important dates
Deadline for paper submission: April 7th, 2006
Deadline for panel submission: April 22nd, 2006
Notification of acceptance or rejection: June 5th, 2006
Final paper camera-ready copy due: June 21st, 2006
Deadline for Student Scholarships: July 30th, 2006
Notification for Student Scholarships: August 4th, 2006
Deadline for poster abstract submission: August 6th, 2006
Notification for poster acceptance: August 14th, 2006

Ongoing Call for Participation and Poster Proposals
This symposium, the ninth in an annual series, brings together leading researchers and practitioners from academia, government, and industry to discuss issues and technologies related to intrusion detection and defense. The Recent Advances in Intrusion Detection (RAID) International Symposium series is intended to further advances in intrusion defense by promoting the exchange of ideas in a broad range of topics.

This year, the RAID program includes sixteen full presentations selected from almost 100 submissions, with proceedings published by Springer. The program also includes invited speakers and a poster session. RAID will accept poster submissions until August 6th.
The RAID organizing committee calls for the participation of the global IT security professional and research communities.

Preliminary Program
Wednesday, September 20th, 2006: Registration starts at 9:00
12:30–14:00 Lunch
14:00–14:15 Welcome to RAID 2006
14:15–15:15 Invited Talk
15:45–16:45 Session: Anomaly Detection
A Framework for the Application Of Association Rule Mining In Large Intrusion Detection Infrastructures
James J. Treinen and Ramakrishna Thurimella
Behavioral Distance Measurement Using Hidden Markov Models
Debin Gao, Michael K. Reiter, and Dawn Song
17:00–18:00 Poster abstract session (5-minute talks)
18:00–20:00 Poster session
Thursday, September 21st, 2006
09:00–10:30 Session: Attacks
Automated Discovery of Mimicry Attacks
Jonathon T. Giffin, Somesh Jha, and Barton P. Miller
Allergy Attack Against Automatic Signature Generation
Simon P. Chung and Aloysius K. Mok
Paragraph: Thwarting Signature Learning By Training Maliciously
James Newsome, Brad Karp, and Dawn Song
11:00–12:30 Session: System Evaluation and Threat Assessment
Anomaly Detector Performance Evaluation Using A Parameterized Environment
Jeffery P. Hansen, Kymie M.C. Tan and Roy A. Maxion
Ranking Attack Graphs
Vaibhav Mehta, Constantinos Bartzis, Hai Feng Zhu, Edmund Clarke, and Jeanette Wing
Using Hidden Markov Models to Evaluate The Risks Of Intrusions–System Architecture And Model Validation
Andre Arnes, Fredrik Valeur, Giovanni Vigna, and Richard A. Kemmerer
12:30–14:00 Lunch
14:00–15:00 Invited Talk
15:30–17:00 Session: Malware Collection and Analysis
The Nepenthes Platform: An Efficient Approach To Collect Malware
Paul Baecher, Markus Koetter, Thorsten Holz, Maximillian Dornseif, and Felix Freiling
Automatic Handling of Protocol Dependencies & Reaction To 0-Day Attacks With ScriptGen-Based Honeypots
Corrado Leita, Marc Dacier, and Frederic Massicotte
Fast and Evasive Attacks: Highlighting The Challenges Ahead
Mohede Abu Rajab, Fabian Monrose, and Andreas Terzis
Friday, September 22nd, 2006
09:00–10:00 Session: Anomaly- and Specification-Based Detection
Anagram: A Content Anomaly Detector Resistant to Mimicry Attack
Ke Wang, Janak J. Parekh, and Salvatore J. Stolfo
DEMEM: Distributed Evidence-Driven Message Exchange Intrusion Detection Model for MANET
Chinyang Henry Tseng, Shiu-Huey Wang, Calvin Ko, and Karl Levitt
10:30–12:00 Session: Network Intrusion Detection
Enhancing Network Intrusion Detection with Integrated Sampling and Filtering
Jose M. Gonzalez and Vern Paxson
WIND: Workload-Aware Intrusion Detection
Sushant Sinha, Farnam Jahanian, and Jignesh M. Patel
12:00–12:15 Concluding remarks

Organizing Committee
General Chairs: Dieter Gollmann (Technical University Hamburg-Harburg, diego@gollmann-harburg.de), Andreas Frauenhi-Jstech)
Program Chair: Diego Zamboni (IBM Zurich Research Laboratory, dza@zurich.ibm.com)
Publication Chair: James Riordan (IBM Zurich Research Laboratory, rjord@zurich.ibm.com)
Publicity Chair: Robert Cunningham (MIT Lincoln Laboratory, rke@ll.mit.edu)
Sponsorship Chair: Klaus-Peter Kossakovski (PRESECURE Consulting, kpk@gse-security.de)

Steering Committee
Chair: Marc Dacier (Eurowecom, France)
Herve Debar (France Telecom R&D, France)
Deborah Frincke (Pacific Northwest National Lab, USA)
Ming-Yah Huang (The Boeing Company, USA)
Erland Jonsson (Chalmers, Sweden)
Kwok-Tung Wong (Chinese University of Hong Kong, China)
Kees van Reeuwijk (TNO, The Netherlands)
Wolfgang Nejdl (Max-Planck Institute for Informatics, Germany)
Kees van der Schaft (IBM Zurich Research Laboratory, kvs@zurich.ibm.com)
Kris Yokoyama (IBM Tokyo Research Laboratory, kyoko@ibm.co.jp)

Important dates
Deadline for paper submission: April 7th, 2006
Deadline for panel submission: April 22nd, 2006
Notification of acceptance or rejection: June 5th, 2006
Final paper camera-ready copy due: June 21st, 2006
Deadline for Student Scholarships: July 30th, 2006
Notification for Student Scholarships: August 4th, 2006
Deadline for poster abstract submission: August 6th, 2006
Notification for poster acceptance: August 14th, 2006

Corporate Sponsors
The RAID committee would like to thank the Northwest Security Institute (NWSI) for providing funding for student scholarships. We solicited interested organizations to serve as sponsors for RAID 2006, particularly in sponsorship of student travel and other expenses for RAID. Please contact the Sponsorship Chair for information regarding corporate sponsorship of RAID 2006. For further information, please visit the RAID web site or contact the Program Chair or the General Chair.