RAID 2008 Program

All sessions are at the Tang Conference Center on the MIT Campus in Cambridge, MA. Breakfast and lunch are provided as well as a Boston Duck Boat Tour and Dinner at the Top of the Hub. Wireless internet connections will be available.

Monday, 15 September 2008

1:00 – 7:00 PM  RAID registration
1:00 – 5:30 PM  Poster Setup
5:30 – 8:00 PM  Joint Catered Poster Session with VizSEC

Tuesday, 16 September

8:00 – 9:00 AM  Breakfast (Ting Foyer in Tang Conference Center) and Registration
9:00 – 9:15 AM  Welcome – Robert Cunningham RAID 2008 General Chair
                Conference Opening – Richard Lippmann RAID 2008 Program Chair

Session 1  Rootkit Prevention
9:15 – 10:00 AM Chair: Thorsten Holz
               Guest-Transparent Prevention of Kernel Rootkits with VMM-based Memory Shadowing
               Ryan Riley (Purdue University, US); Xuxian Jiang (George Mason University, US);
               Dongyan Xu (Purdue University, US)
               Countering Persistent Kernel Rootkits Through Systematic Hook Discovery Zhi Wang
               (George Mason University, US); Xuxian Jiang (George Mason University, US); Weidong
               Cui (Microsoft Research, US); Xinyuan Wang (George Mason University, US)

10:00 – 10:30 AM Break

10:30 – 12:00 Noon Moderator: Robert Cunningham, MIT Lincoln Laboratory
               Panel Members: Jacques Bus, Head of Unit: Security - ICT Programme European
               Commission; Carl Landwehr, Program Manager, IARPA; Karl Levitt, Cyber Trust
               Program Director, National Science Foundation; Doug Maughan, Program Manager of
               Cyber Security R&D, Department of Homeland Security

12:00 – 1:30 PM Lunch (MIT Faculty Club)

Session 2  Malware Detection and Prevention
1:30 – 3:00 PM Chair: Engin Kirda
               Tamper-Resistant, Application-Aware Blocking of Malicious Network Flows Abhinav
               Srivastava (Georgia Institute of Technology, US); Jonathon Giffin (Georgia Institute of
               Technology, US)
               A First Step Toward Live Botmaster Traceback Daniel Ramsbrock (George Mason
               University, US); Xinyuan Wang (George Mason University, US); Xuxian Jiang (George
               Mason University, US)
A Layered Architecture for Detecting Malicious Behaviors Lorenzo Martignoni (University of Milan, IT); Elizabeth Stinson (Stanford University, US); Matt Fredrikson (University of Wisconsin, Madison, US); Somesh Jha (University of Wisconsin, US); John Mitchell (Stanford University, US)

A Study of the Packer Problem and Its Solutions Fanglu Guo (State University of New York at Stony Brook, US); Tzi-Cker Chiueh (State University of New York at Stony Brook, US)

3:00 – 3:30 PM Break

Session 3 High Performance Intrusion Detection and Evasion
3:30 – 5:00 PM Chair: Ulrich Flegel

Gnort: High Performance Network Intrusion Detection Using Graphics Processors Giorgos Vasiliadis (Institute of Computer Science, Foundation for Research and Technology Hellas, GR); Spiros Antonatos (Institute of Computer Science, Foundation For Research and Technology Hellas, GR); Michalis Polychronakis (ICS-FORTH, GR); Evangelos Markatos (ICS-FORTH, GR); Sotiris Ioannidis (University of Crete, GR)

Predicting the Resource Consumption of Network Intrusion Detection Systems Holger Dreger (Siemens AG, DE); Anja Feldmann (Deutsche Telekom Laboratories, DE); Vern Paxson (ICSI, US); Robin Sommer (ICSI and LBNL, US)

High-speed Matching of Vulnerability Signatures Nabil Schear (University of Illinois at Urbana-Champaign, US); David Albrecht (University of Illinois at Urbana-Champaign, US); Nikita Borisov (University of Illinois at Urbana Champaign, US)

Inefficient Attacks against Network-level Emulation/Analysis Simon Pak Ho Chung (University of Texas at Austin, US); Aloysius Mok (University of Texas at Austin, US)

5:15 PM Climb on Board Duck Boats for Tour and Dinner at the Top of the Hub. Attendees return to their hotels via the "T", cab, or walking.

Wednesday, 17 September

8:00 – 9:00 AM Breakfast (Ting Foyer in Tang Conference Center) and Registration

9:00 – 9:15 AM Announcements

Session 4 Web Application Testing and Evasion
9:15 – 10:00 AM Chair: Jon Giffin

Leveraging User Interactions for In-Depth Testing of Web Applications Sean McAllister (Technical University Vienna, AT); Engin Kirda (Institute Eurecom, FR); Christopher Kruegel (University of California, Santa Barbara, US)

Model-Based Covert Timing Channels: Automated Modeling and Evasion Steven Gianvecchio (The College of William & Mary, US); Haining Wang (College of William and Mary, US); Duminda Wijesekera (George Mason University, US); Sushil Jajodia (George Mason University, US)
10:00 – 10:30 AM Break

Panel 2 Life After Antivirus – What Does the Future Hold?
10:30 – 12:00 Noon Moderator: Richard Lippmann, MIT Lincoln Laboratory


12:00 – 1:30 PM Lunch (MIT Faculty Club)

Session 5 Alert Correlation and Worm Detection
1:30 – 3:00 PM Chair: Benjamin Morin

Optimal Cost, Collaborative and Distributed Response to Zero-Day Worms -- A Control Theoretic Approach Senthil Cheetancheri (University of California, Davis, US); John Agosta (Intel Research, US); Karl Levitt (UC Davis, US); S. Felix Wu (University of California at Davis, US); Jeff Rowe (UC Davis, US)

On the limits of payload-oblivious network attack detection Michael Collins (CERT, US); Mike Reiter (University of North Carolina at Chapel Hill, US)

Determining placement of intrusion detectors for a distributed application through Bayesian network modeling Gaspar Modelo-Howard (Purdue University, US); Saurabh Bagchi (Purdue University, US); Guy Lebanon (Purdue University, US)

A Multi-Sensor Model to Improve Automated Attack Detection Magnus Almgren (Chalmers University of Technology, SE); Ulf Lindqvist (SRI International, US); Erland Jonsson (Chalmers University of Technology, SE)

3:00 – 3:30 PM Break

Session 6 Anomaly Detection and Network Traffic Analysis
3:30 – 5:00 PM Chair: Robin Sommer

Monitoring SIP traffic using Support Vector Machines Mohamed Nassar (INRIA Lorraine, FR); Radu State (INRIA - LORIA, FR); Olivier Fester (INRIA-LORIA, FR)

The Effect of Clock Resolution on Keystroke Dynamics Kevin Killourhy (Carnegie Mellon University, US); Roy A. Maxion (Carnegie Mellon University, US)

A Comparative Evaluation of Anomaly Detectors under Portscan Attacks Ayesha Binte Ashfaq; Maria Joseph; Asma Mumtaz; Muhammad Qasim Ali; Ali Sajjad; Syed Ali Khayam (National University of Sciences & Technology, PK)

Advanced Network Fingerprinting Humberto Abdelnur (INRIA Nancy - Grand Est, FR); Radu State (INRIA - LORIA, FR); Olivier Fester (INRIA Nancy - Grand Est, FR)

5:00 PM Conference Ends

The RAID organizing committee would like to thank our sponsors:
The I3P, IBM, MIT Lincoln Laboratory and Symantec.