

Completion report for RNSA Network Monitoring



Event : RNSA Network Monitoring

Location : Crowne Plaza, Surfers Paradise Hotel, Gold Coast

Date : 4 September 2007

Summary Leading researchers and security professionals from overseas and Australia gathered at the Gold Coast for RAID – Recent Advances in Intrusion Detection – in September 2007. Immediately prior to RAID, with the support of the Research Network for a Security Australia (RNSA), Queensland University of Technology’s Information Security Institute organised a workshop for academic, industry and government participants focusing on challenges and leading edge activities in the area of network threat monitoring. The workshop featured several distinguished presenters from Europe, North America, and Australia.

Event rationale This event was supported by the RNSA because it contributed to the RNSA mission statement of *facilitating a knowledge-sharing network for research organisations, government and the private sector to develop research tools and methods to mitigate emerging safety and security issues.* A number of excellent contacts were made between the participants and speakers.

Number of attendees The attendees consisted of
12 paying attendees
20 complimentary registrations

Financial details

Income from registrants	
12 Delegates (\$350 each)	\$4,200

Expenses	
22 hours staff support (E Geoghegan & Athol Yates)	\$1,540
- Registrations	
- Website update	
- Email out	
- Delegate enquiries	
Total	\$1,540

Profit and loss	
Income	\$4,200
Expenses	\$1,540
Profit	\$2,660

All figures include GST

Attachments

Attachment 1 contains the program.
Attachment 2 contains the list of delegates and speakers.

Information

Athol Yates
Outreach Manager, RNSA
rnsa@homelandsecurity.org.au

Attachment 1: Program

08:15 Registration, Coffee/Tea

SESSION 1

08:55 Opening Address - Ed Dawson (QUT)

09:00 Network Monitoring – Operational Challenges - Graham Ingram (AusCERT, Australia)

09:45 Host and Subnet Behaviours: Visualization for Measurement and Insight - John McHugh (Dalhousie University, Canada)

10:30 Morning Tea

SESSION 2

11:00 Leurré.com V2.0: Beyond Low Interaction Honeypots - Marc Dacier (Institute Eurécom, France)

11:45 Analyzing Malicious Code - Christopher Kruegel (Technical University Vienna, Austria)

12:30 Lunch

SESSION 3

13:30 Monitoring a Network Service without Knowing the Threat - Ludovic Mé (Supélec, France)

14:15 Cybersecurity and Critical Information Infrastructure Protection - Olivier De Vel (DSTO, Australia)

15:00 True Challenges of 21st Century Information Security R&D - Ming-Yuh Huang (The Boeing Company, USA)

15:45 Afternoon Tea

PANEL SESSION

16:15 Application Security is all that Matters

17:00 Close

Attachment 3: List of attendees and speakers

Involvement	Title	First Name	Surname	Position	Organisation	Email	Phone
	Mr					n.sharma@griffith.edu.au	
Delegate	Mr	Olivier	Thonnard	PhD student	Royal Military Academy	olivier.thonnard@ibelgique.com	+3227426510
Delegate	Mr	Robin	Sommer		ICSI/LBNL	robin@icsi.berkeley.edu	1-510-666-2886
Delegate	Mr	Benjamin	Morin		Supelec	benjamin.morin@supelec.fr	+33)299844500
Delegate	Mr	Anthony	Wein	Assistant Director, GovCERT.au	Attorney-General's Department	tony.wein@ag.gov.au	02 6272 7131
Delegate	Mr	ANWAR DEEN	TOUREY	MARKETING MANAGER	AABSLOW COMPLEX GHANA LTD	one_x72000@yahoo.com	+4793064908
Delegate	Mr	Arne	Ostebo	Scientist	UNINETT	arneos@uninett.no	0011 1 703-983-3242
Delegate	Mr	Greg	Stephens	Principal Infosec Engineer	The MITRE Corporation	gstephens@mitre.org	0011 1 781 981-2711
Delegate	Dr	Richard	Lippmann	Senior Staff	MIT Lincoln Laboratory	LIPPMANN@LL.MIT.EDU	
Delegate - Complimentary	Mr	Graham	Ingram	General Manager	AusCERT	graham@auscert.org.au	07 33654417
Delegate	Mr	Matthew	Aburn	Security Analyst Manager, Analysis & Assessments	AusCERT	maburn@auscert.org.au	07 33654417
Delegate	Ms	Kathryn	Kerr	Associate Director, ICTS	AusCERT	kathryn@auscert.org.au	07 33654417
Delegate	Mr	Naveen	Sharma		Griffith University	N.Sharma@griffith.edu.au	07 3735 7601
Delegate	Mr	Ludovic	Me		Supelec	ludovic.me@supelec.fr	(+33)299844500
Delegate - Complimentary	Mr	Steven	Panichprecha		Queensland University of Technology		
Delegate - Complimentary	Mr	Saleh	Almotairi		Queensland University of Technology		
Delegate - Complimentary	Mr	Mal	Corney		Queensland University of Technology		
Delegate - Complimentary	Mr	Jason	Smith		Queensland University of Technology	smith@isrc.qut.edu.au	07 1815 9361
Delegate - Complimentary	Dr	Jacob	Zimmermann		Queensland University of Technology		
Delegate - Complimentary	Professor	Ed	Dawson	Director	Queensland University of Technology	e.dawson@qut.edu.au	07 3864 9551

Delegate - Complimentary	Mr	Mehdi	Kiani Harchegani	Queensland University of Technology Defence Science and Technology Organisation (DSTO)	Olivier.DeVel@dsto.defence.gov.au
Delegate - Complimentary	Dr	Olivier	de Vel	Queensland University of Technology	07 3138 9550
Delegate - Complimentary	Dr	Andrew	Clark	Queensland University of Technology	a.clark@qut.edu.au
Delegate - Complimentary	Mr	Andrew	Marrington	Queensland University of Technology	a.marrington@qut.edu.au
Delegate - Complimentary	Mr	Ejaz	Admed	Queensland University of Technology	
Delegate - Complimentary	Mr	Vic Tor	Goh	Queensland University of Technology	
Delegate - Complimentary	Mr	Graham	Ingram	AusCERT, Australia	
Delegate - Complimentary	Prof	John	McHugh	Dalhousie University, Canada	
Delegate - Complimentary	Prof	Marc	Dacier	Institute Eurecom, France	
Delegate - Complimentary	Prof	George	Mohay	Queensland University of Technology	
Delegate - Complimentary	Prof	Ludovic	Me	Supelec, France	
Delegate - Complimentary	Dr	Ming-Yuh	Huang	The Boeing Company, USA	
Delegate - Complimentary	Prof	Christopher	Kruegel	Technical University Vienna, Austria	



RNSA Workshop

Networking Monitoring: Identifying and Measuring the Threat

This one-day workshop is being presented by the Information Infrastructure Security Hub of the RNSA and will be held at

**Crowne Plaza Surfers Paradise Hotel,,
Pacific Highway, Surfers Paradise, Gold Coast, Qld. Australia**

Tuesday, 4th September, 2007

For map of Crowne Plaza Surfers Paradise Hotel, please visit:
<http://www.rydges.com/riverwalk>

Nominations to attend by 28 August, 2007

Overview

Leading researchers and security professionals from overseas and Australia will be gathered at the Gold Coast for RAID – *Recent Advances in Intrusion Detection* – in September 2007. Immediately prior to RAID, with the support of the Research Network for a Security Australia (RNSA), Queensland University of Technology's Information Security Institute is organising a workshop for academic, industry and government participants focusing on challenges and leading edge activities in the area of network threat monitoring. The workshop features several distinguished presenters from Europe, North America, and Australia. Full program details, along with presenter biographies and abstracts can be found below. Registration details are also provided.

Program

08:15 Registration, Coffee/Tea

SESSION 1

08:55 *Opening Address*
Ed Dawson (QUT)

09:00 *Network Monitoring – Operational Challenges*
Graham Ingram (AusCERT, Australia)

09:45 *Host and Subnet Behaviours: Visualization for Measurement and Insight*
John McHugh (Dalhousie University, Canada)

10:30 Morning Tea

SESSION 2

11:00 *Leurre.com V2.0: Beyond Low Interaction Honeypots*
Marc Dacier (Institute Eurécom, France)

11:45 *Analyzing Malicious Code*
Christopher Kruegel (Technical University Vienna, Austria)

12:30 Lunch

SESSION 3

13:30 *Monitoring a Network Service without Knowing the Threat*
Ludovic Mé (Supélec, France)

14:15 *Cybersecurity and Critical Information Infrastructure Protection*
Olivier De Vel (DSTO, Australia)

15:00 *True Challenges of 21st Century Information Security R&D*
Ming-Yuh Huang (The Boeing Company, USA)

15:45 Afternoon Tea

PANEL SESSION

16:15 *Application Security is all that Matters*

17:00 Close

Organisation

This event is organised by the Research Network for a Secure Australia (RNSA). RNSA is a multi-disciplinary collaboration established to strengthen Australia's research capacity for protecting critical infrastructure from natural or other disasters. The RNSA facilitates a knowledge-sharing network for research organisations, government and the private sector to develop research tools and methods to address emerging safety and security issues relating to critical infrastructure. World-leaders with extensive national and international linkages in relevant scientific, engineering and technological research will lead this collaboration. The RNSA also organises various activities to foster research collaboration and nurture young investigators.

Eligible participants are encouraged to join the RNSA. Membership of the RNSA which is open to Australian and international researchers, industry, government and others professionally involved in CIP Research. Information on joining is at <http://www.secureaustralia.org/>.

Registration and Costs

RNSA members: AUD \$300.00

Non RNSA members: AUD \$350.00

Registration and payment can be made "on line" at:

<https://anchor.net.au/secure/homelandsecurity.org.au/ahs/register.php?id=121>

Morning Tea, Lunch and Afternoon Tea are included in the registration cost.

Limited financial support is available for academic members of RNSA (who also attend RAID) to cover airfares and/or accommodation. Interested Persons should contact Mr Elizabeth Hansford (email: e.hansford@qut.edu.au, phone: (07) 3138 9573)

Registration will be accepted up to 28 August, 2007

For Information

Elizabeth Hansford

Administration Manager

Information Security Institute

Queensland University of Technology

GPO Box 2434 (126 Margaret Street

Brisbane, Qld. 4001

Tel: (07) 3138 9573 Fax: (07) 3221 2384

Email: e.hansford@qut.edu.au

Abstracts and Speaker Bios

Network Monitoring – Operational Challenges

Graham Ingram, AusCERT, Australia

Abstract: Current trends in the ways both malicious and legitimate traffic are using networks lead to challenges for practical network monitoring. This presentation reviews the nature of the threat, current trends and their implications for current and future monitoring systems.

Insight into likely responses by online criminals to more widespread network monitoring can be gained from the similar escalation of technology observed between banks and criminals in the past few years.

Beyond protection of the corporate border, there is a need for a collaborative response to information from network monitoring systems. Building this social and technical infrastructure is work in which AusCERT and its international partners are currently engaged.

Bio: Graham Ingram is the General Manager of AusCERT. He took up the position in January 2002 after 17 years employment with the Australian government. Immediately prior to joining AusCERT, Graham worked with the Australian Department of Defence where he was responsible for managing computer security incident reporting and response for Commonwealth government agencies.

Graham has extensive experience in critical information infrastructure protection (CIP) and spent four years working in this area for the government. During this period he managed a number of major IT security and information protection issues including computer network attacks during the Y2K period and IT security threats to the 2000 Olympic games.

Since joining AusCERT, Graham has consolidated AusCERT as Australia's national Computer Emergency Response Team (CERT) and strengthened its strategic relationships particularly in the Asia Pacific region. AusCERT was the founding chair of APCERT which comprises the leading 17 CERTs/CSIRTs from 14 economies in the Asia Pacific Region. Graham has a BSc (honours).

Host and Subnet Behaviours: Visualization for Measurement and Insight

John McHugh, Dalhousie University, Canada

Abstract: A few years ago, I was fortunate enough to have access to netflow border data from the boundaries between a very large (but segmented) network and the internet as a whole. This is effectively a very large network telescope. One of the interesting things about data of this sort is that it is possible to work at scales that range from single digit percentages of the IPv4 address space to individual hosts. In optical terms, this is equivalent to having a zoom lens with about a 100 million to one zoom ratio looking inward and a 4 billion to one ratio looking outward (but the outward sky is partly cloudy, so we only see sources that shine through the openings). More recently, my students and I have been analyzing data from smaller networks and we have had the good fortune to look at a small network that has had an interesting set of compromises. From our previous work, we have hypothesized that certain types of visualizations would be useful in understanding the behaviors of individual hosts, as well as subnetworks and have been developing some tools that aid in this understanding. In addition, we also discovered evidence of an emergent phenomenon that can only be seen at the full aperture of the outward looking telescope. In this talk, I will discuss the relationship between our visualizations and the measurements that they enable. While, in principle, it would be possible to achieve these results without the visual component, we claim that using the visualizations helps to direct the quantitative measurements and analyses and improves the efficiency and effectiveness of the analyst.

Bio: John McHugh is a professor and Canada Research Chair in Privacy and Security at Dalhousie University in Halifax, NS where he also directs the Privacy and Security Laboratory. Before joining the faculty at Dalhousie, he was a senior member of the technical staff at the CERT Coordination Center, part of the Software Engineering Institute at Carnegie Mellon University where he did research in survivability, network security, and intrusion detection. He was also affiliated with CyLab and the Center for Wireless and Broadband Research, both part of the Department of Electrical and Computer Engineering at CMU.

Prior to joining CERT, Dr. McHugh was a professor and chairman of the Computer Science Department at Portland State University in Portland, Oregon where he held a Tektronix Professorship. He has been a member of the research faculty at the University of North Carolina and has taught at UNC and at Duke University. For a number of years, Dr. McHugh was a Vice President of Computational Logic, Inc., a contract research company formed to further the application of formal methods of software design and analysis in support of security and safety critical systems. While at CLI, he developed tools for the analysis of covert channels in multilevel secure systems and worked on the problems associated with the efficient implementation of formally specified systems. He has also worked for the Research Triangle Institute, the Naval Research Laboratory, the National Oceanic and Atmospheric Administration, the University of Minnesota, and the U.S. Patent Office.

Dr. McHugh received his PhD degree in computer science from the University of Texas at Austin. He has a MS degree in computer science from the University of Maryland, and a BS degree in physics from Duke University. He is the author of numerous technical papers and reports. He has served as the chair of the IEEE Computer Society's Technical Committee on Security and Privacy and is a member of the advisory board for the International Journal of Information Security. He serves on the program or advisory committees of many of the major conferences and workshops in the computer security field.

Leurré.com V2.0: Beyond Low Interaction Honeypots

Marc Dacier, Institut Eurécom, France

Abstract: For almost four years, we have maintained a worldwide distributed system of low interaction honeypots, based on honeyd. In this presentation, we will report on the lessons learned and the tools developed. We will explain how the research community can get access to the dataset accumulated as well as to the technology created around it. Furthermore, we will describe the future plans for this infrastructure. We are considering the integration of scriptgen, argos and nepenthes to offer a system which would be as powerful as high interaction systems without suffering from their known drawbacks (costs, privacy and liability issues). The overall architecture will be exposed and interested partners will be invited to join us in the beta testing phase of this new system.

Bio: Marc Dacier is a professor at the Eurecom Institute (www.eurecom.fr/dacier). He also is an associate professor at the Université de Liège, in Belgium. From 1996 until 2002, he worked at IBM Research as the manager of the Global Security Analysis Lab. In 1998, he co-founded with K. Jackson the "Recent Advances on Intrusion Detection" Symposium (RAID). He is now chairing its steering committee. He also was the co-director, with first Brian Randell and then Robert Stroud from the University of Newcastle, of the MAFTIA IST ReSIST FP5 Project. He represents Eurecom in the executive board of FP6 RESIST Network of Excellence. He serves on the program committees of major security and dependability conferences and is a member of the steering committee of the "European Symposium on Research for Computer Security" (ESORICS). He is a member of the editorial board of the following journals: IEEE TDSC, ACM TISSEC and JIAS. His research and teaching interests include computer and network security, intrusion detection, network and system management. He is the author of numerous international publications and several patents.

Analyzing Malicious Code

Christopher Kruegel, Technical University Vienna, Austria

Abstract: Malware, such as viruses, worms, or spyware, is defined as software that fulfils the deliberately harmful intent of an attacker when run. To effectively combat malicious code, it is necessary to understand the behaviour of real-world malware programs. To this end, we have deployed both server-side and client-side honeypots that collect malicious programs in the wild. These programs are then forwarded to an automated analysis engine called Anubis. Anubis performs dynamic code analysis to extract the behaviour of malware. In addition to recording a simple execution trace, our system identifies hidden behaviour that is only triggered under certain circumstances (for example, on a certain date, or when the malware program is started in a specific directory). Moreover, Anubis tracks how malware uses data that it reads from operating system resources (such as files or sockets). This provides valuable information about the intent of the malicious program.

Bio: Christopher Kruegel is an assistant professor at the Technical University Vienna in Austria. Before that, he held a post-doctoral researcher position at the University of California, Santa Barbara. Christopher's research is focused on applied computer security, with an emphasis on intrusion detection, malicious code analysis, and web security. He has published more than 50

publications in these areas and regularly serves on the program committees of well-known security conferences. In addition, he served as the program chair for the 10th International Symposium on Recent Advances in Intrusion Detection (RAID) and the 5th ACM Workshop on Recurring Malcode (WORM).

Monitoring a Network Service without Knowing the Threat

Ludovic Mé, Supélec, France

Abstract: When trying to measure and identify the threats against our information systems through network monitoring, are we new alchemist trying to turn lead into gold? If it appears of course possible to learn about cyber-attacks, is it possible to do so sufficiently quickly and efficiently to be able to push back this new knowledge in real time, as new vulnerabilities and exploits appear, in our intrusion detection systems? Of course, we all hope so. However, being able to monitor our information systems without having to know precisely the threat would also be interesting.

In the dependability field, N-version programming is a known method to ensure fault tolerance in highly secure system. It consists in the execution of a single function by two or more elements, called versions, and in the comparison of the results of the different versions to make a decision on the result. The underlying hypothesis is that the different versions used are independent from the point of view of their faults.

This technique has been applied successfully in various projects to provide intrusion detection as well. Each version is viewed by the others as an implicit and complete reference model. We thus have here a form of "anomaly" detection, in which there is no need for an explicit model, as required usually. This is an important advantage as such explicit models are difficult to build.

Two types of approaches have been investigated: the black-box approach that consists in comparing the outputs of several COTS implementing the same service, and the gray-box approach that requires an intrusive observation of the activities that occur on the diversified servers, to allow for example the comparison of information flow graphs generated by these activities. In both approaches, the masking of "known anomalies" is mandatory, as the different COTS services may respond differently to the same request. For that purpose, a small and easy-to-build explicit model of differences is required.

Compared to the black-box approach, the gray-box approach increases the detection coverage of various class of attacks and presents an interesting advantage for an anomaly detector: it provides a diagnosis of the alerts emitted by the intrusion detection system. As such, it can be viewed as a way to identify the threat against our information systems.

Bio: Ludovic Mé (www.rennes.supelec.fr/rennes/si/equipe/lme) graduated from Supélec and from the Rennes University (PhD, 94). He has been teaching in Supélec since 1988, where he is currently Professor, head of the "Network and Information System Security" group. His research interests focus on intrusion detection and spontaneous network security. He seats at the RAID symposium (Recent Advances in Intrusion Detection) steering comity and has also served numerous international conference program comities. He authored or co-authored more than 30 international communications.

Cybersecurity and Critical Information Infrastructure Protection

Olivier De Vel, DSTO, Australia

Abstract: We describe an advanced AI-based system developed for the monitoring and control of ultra-large networks in near real-time. We also present extensions of this system as applied to different areas of critical information infrastructure protection.

Bio: Olivier de Vel is Research Leader in the Information Assurance Branch in the Command, Control, Communications and Intelligence Division at DSTO. The Branch undertakes R&D in information security, identity management, computer network defence, digital forensics, special security devices and high assurance systems. Olivier obtained an MSc(Hons) at University of Waikato (New Zealand) and a PhD in 1978 from the Institut National Polytechnique de Grenoble (France). He has been at DSTO since 1999 and his research interests are in the application of learning machines to computer security.

True Challenges of 21st Century Information Security R&D

Ming-Yuh Huang, The Boeing Company, USA

Abstract: Today's information security is no longer about keeping people out; it's about letting people in - the right people, the right time, to the right resources. Modern social and business practices require us to work closely together via access to the computing infrastructure and the Internet. Once connected, each needs to be brought directly to the right resources. In this respect, information security today is the key "business-enabler" that propels the next-generation paradigm shift. Traditional way of looking at information security as a protecting and prohibiting technology is out of date. Boeing operates one of the largest computing infrastructures in the world executing complex global manufacturing, distributed collaborative engineering, massive virtual enterprise integration, as well as building highly complex large-scale defense and government systems. In this context, I like to share our perspectives on 21st century information security R&D issues and directions - what's catch-up vs. what's enabling, what's relevant vs. what's irrelevant.

Bio: Ming-Yuh Huang (who goes by "Huang") is a Boeing Fellow leading Boeing's Information Assurance R&D Program to support the corporate enterprise as well as a wide array of large-scale commercial/military programs. Before joining Boeing in 1990, Huang was with DEC Research Artificial Intelligence Technology Center leading an expert system effort called ESSENSE (Expert System for Service Network Security) which led to one of world's earliest intrusion detection products - POLYCENTER ID. While with Boeing, Huang had led DARPA intrusion detection R&D project, co-authored IETF standard IDMEF Intrusion Detection Systems communication protocol in collaboration with IBM Research and US Air Force Information Warfare Center. He was the program-co-chair of RAID-1999 (International Symposium on Recent Advances in Intrusion Detection) at Purdue, and the general-chair of RAID-2005 at Seattle. He was also the program-chair of NATO Advanced Research Workshop "Cyber Security and Defense: Research Issues" at Gdansk, Poland in 2005, and the program-chair of SADFE-2005 (Systematic Approaches to Digital Forensic Engineering) at Taipei, Taiwan. Huang was thrice invited by European Commission & US National Science Foundation to help defining US/EU information security R&D collaboration framework. Huang received his B.S. in Physics in 1979; received MS in Computer Science

