

Thursday, 6th September, 2007

Session 4:

09:00 – 10:30

NETWORK-BASED INTRUSION DETECTION AND RESPONSES

Chair: Giovanni Vigna

- ***Emulation-Based Detection of Non-self-contained Polymorphic Shellcode***
Michalis Polychronakis, Kostas G. Anagnostakis, and Evangelos P. Markatos
- ***The NIDS Cluster: Scalable, Stateful Network Intrusion Detection on Commodity Hardware***
Matthias Vallentin, Robin Sommer, Jason Lee, Craig Leres, Vern Paxson, and Brian Tierney
- ***Cost-Sensitive Intrusion Responses for Mobile Ad Hoc Networks***
Shiau-Huey Wang, Chinyang Henry Tseng, Karl Levitt, and Matthew Bishop

10:30 – 11:00

Morning Tea

Session 5

11:00 – 12:00

INSIDER DETECTION AND ALERT CORRELATION

Chair: Richard Lippmann

- ***ELLICIT: A System for Detecting Insiders Who Violate Need-to-know***
Marcus A. Maloof and Gregory D. Stephens
- ***On the Use of Different Statistical Tests for Alert Correlation - Short Paper***
Federico Maggi and Stefano Zanero

12:00 – 13:30

Lunch

Session 6:

13:30 – 15:00

MALICIOUS CODE ANALYSIS

Chair: Thorsten Holz

- ***Automated Classification and Analysis of Internet Malware***
Michael Bailey, Jon Oberheide, Jon Andersen, Z. Morley Mao, Farnam Jahanian, and Jose Nazario
- ***'Out-of-the-box' Monitoring of VM-based High-Interaction Honeypots***
Xuxian Jiang and Xinyuan Wang
- ***A Forced Sampled Execution Approach to Kernel Rootkit Identification***
Jeffrey Wilhelm and Tzi-cker Chiueh

15:00 – 15:30

Afternoon Tea

Session 7:

15:30 – 16:30

EVASION

Chair: Robin Sommer

- ***Advanced Allergy Attacks: Does a Corpus Really Help?***
Simon P. Chung and Aloysius K. Mok
- ***Alert Verification Evasion through Server Response Forging***
Adam D. Todd, Richard A. Raines, Rusty O. Baldwin, Barry E. Mullins, and Steven K. Rogers

18:15 Drinks

19:00 Dinner

Conference Dinner – “Norfolk Room”

with ***Nahri Dance/Didgeridoo Entertainers***



Friday, 7th September, 2007

09:00 – 10:00

Keynote Address, Chair: Christopher Kruegel
National Information Infrastructure Protection (NIIP) and the Role of IDS
Professor Emeritus Bill Caelli, AO

10:00 – 10:30

Morning Tea

Session 8:

10:30 – 12:00

MALICIOUS CODE DEFENSE

Chair: Ludovic Me

- ***Hit-List Worm Detection and Bot Identification in Large Networks Using Protocol Graphs***
M. Patrick Collins and Michael K. Reiter
- ***SpyShield: Preserving Privacy from Spy Add-ons***
Zhuowei Li, XiaoFeng Wang, and Jong Youl Choi
- ***Vortex: Enabling Cooperative Selective Wormholing for Network Security Systems***
John R. Lange, Peter A. Dinda, and Fabian E. Bustamante

12:00 – 12:15

Concluding Remarks

12:15

Lunch. End of Symposium

