DIMVA 2008 Program

Thursday, July 10th, 2008	
08:30	Registration
09:00	Opening remarks
09:15	Session: Malware detection and prevention (I) (chair: Ludovic Me)
	Dynamic Binary Instrumentation-based Framework for Malware (Virus) Defense, Najwa Aaraj, Anand Raghunathan, Niraj K. Jha Embedded Malware Detection using Markov n-grams, M. Zubair Shafiq, Syed Ali Khayam, Muddassar Farooq Learning and Classification of Malware Behavior, Konrad Rieck, Thorsten Holz, Carsten Willems, Patrick Düssel, Pavel Laskov
10:45	Coffee break
11:15	Session: Attack prevention (chair: John McHugh)
	Data Space Randomization, Sandeep Bhatkar, R. Sekar XSS-GUARD: Precise Dynamic Prevention of Cross-Site Scripting Attacks, Prithvi Bisht, V.N. Venkatakrishnan VeriKey: A Dynamic Certificate Verification System for Public Key Exchanges, Brett Stone-Gross, David Sigal, Rob Cohn, John Morse, Kevin Almeroth, Christopher Kruegel
12:45	Lunch
14:00	Keynote talk: "The Future of Network Security Monitoring", Richard Bejtlich, Director of Incident Response, General Electric
	Abstract: Richard Bejtlich explored Network Security Monitoring (NSM) in his first book, the Tao of Network Security Monitoring: Beyond Intrusion Detection, in 2004. Richard based his discussion on a historical foundation reaching back to the early 1990s. In this talk, Richard will briefly explore that history and provide context for current NSM implementations. Richard will then look forward to see how NSM fits in a world where the cloud is the computer, most endpoints are terminals (again), and the network is one of many simultaneous connections not under control of the IT department.
15:15	Coffee break
15:45	Session: Attack techniques and Vulnerability assessment (chair: Ulrich Flegel)
	On Race Vulnerabilities in Web Applications, Roberto Paleari, Davide Marrone, Danilo Bruschi, Mattia Monga, On the Limits of Information Flow Techniques for Malware Analysis and Containment, Lorenzo Cavallaro, Prateek Saxena, R. Sekar,

DIMVA 2008 Program

Friday, July 11th, 2008	
08:30	Registration
09:00	Keynote talk: "From Virtual Machines to Virtual Infrastructure: How Virtualization is Reshaping the Enterprise and What this Means for Security", Tal Garfinkel, VMware/Stanford University
	Abstract: The move to virtual machine based computing platforms is perhaps the most significant change in how enterprise computing systems have been built in the past decade. In this talk Tal Garfinkel will look at how virtualization is reshaping the way that enterprise data centers are built and managed. He will then share some of the challenges and surprises encountered along the way. Finally, he will explore the unique opportunities these changes are offering to rethink how we design host and network security.
10:15	Coffee break
10:45	Session: Malware detection and prevention (II) (chair: Sven Dietrich)
	Expanding Malware Defense by Securing Software Installations, Weiqing Sun, R. Sekar, Zhenkai Liang, V.N. Venkatakrishnan, FluXOR: detecting and monitoring fast-flux service networks, Emanuele Passerini, Roberto Paleari, Lorenzo Martignoni, Danilo Bruschi Traffic Aggregation for Malware Detection, Ting-Fang Yen, Michael Reiter
12:15	Lunch
13:45	Rump session (chair: Sven Dietrich)
14:45	Coffee break
15:15	Session: Intrusion detection and Activity correlation (chair: Bernhard Haemmerli)
	The Contact Surface: A Technique for Exploring Internet Scale Emergent Behaviors, Carrie Gates, John McHugh The Quest for Multi-headed Worms, Van-Hau Pham, Marc Dacier, Guillaume Urvoy-Keller, Taoufik En-Najjary A Tool for Offline and Live Testing of Evasion Resilience in Network Intrusion Detection Systems (Extended Abstract), Leo Juan, Christian Kreibich, Chih-Hung Lin, Vern Paxson
16:45	Concluding remarks