WRAITS Guest Talk: “Empirical Studies in Cybersecurity”

Michel Cukier
Associate Professor
University of Maryland, College Park, USA

Abstract:

This talk discusses how cybersecurity data (e.g., incidents, intrusion detection system alerts, network flows and malicious activity against a large range of honeypots) can be analyzed to evaluate the security of organizational networks. Since data are highly sensitive, organizations are reluctant to share them. In many organizations, the security team who can collect such data is not willing to share them even within the organization. The University of Maryland (UMD) plays a significant role in cybersecurity research due to a collaboration between the Office of Information Technologies (OIT) security team and UMD researchers. The result of the collaboration is access to and analysis of all security related data collected on UMD networks.

The talk will review some studies conducted using the data provided by OIT. First, organizations face increasing challenges in addressing and preventing computer and network security incidents. Being able to understand and predict trends in incidents can aid an organization’s ability to allocate resources for the prevention of such incidents, as well as the evaluation of mitigation strategies. We compared non-homogeneous Poisson process software reliability growth models and time series models with a large set of security incident data. Based on the over 12,000 incidents recorded since 2001, these models were compared for their prediction capability for the number of incidents.

Second, security administrators lack network visibility, i.e., they often do not have the tools to monitor their networks in detail. Even though about 40,000 IP addresses are linked to UMD users, the UMD network consists of more than 130,000 IP addresses. We developed a tool called Nfsight that identifies clients, servers, and scanners solely based on network flows. Various heuristics have been applied and combined using a Bayesian method. Nfsight is currently monitoring the UMD network and the security team has integrated Nfsight into their security tool suite. Nfsight has found compromised computers that were undetected by the other security tools used by the security team.

Biography:

Michel Cukier is an Associate Professor of Reliability Engineering with a joint appointment in the Department of Mechanical Engineering and the Institute for Systems Research at the University of Maryland, College Park. He is affiliated to the Department of Electrical and Computer Engineering and the Department of Computer Science at the University of Maryland, College Park. He is the PI of an NSF REU Site on cybersecurity in collaboration with Women in Engineering where over 85% of the participants are female students. He co-advises the UMD Cybersecurity Club with a membership of over 300 students.

Dr. Cukier’s research interests include dependability and security validation, dependable and secure computing. In particular, he conducted empirical research studies using security related data. He has published more than 60 technical papers in these areas. He is the Program Chair of ISSRE 2010 and of DSN-PDS 2012.
WRAITS Program

5th Workshop on Recent Advances in Intrusion-Tolerant Systems (WRAITS)

Monday – June 27th, 2011

Introduction .................................................................................................................. 1
Alysson Bessani (University of Lisboa, Portugal), Partha Pal (BBN Technologies, USA)

Session 1: Distributed Systems

The Time-Free Approach to Byzantine Failure Detection in Dynamic Networks .................................................. 3
Murilo Santos de Lima, Fabiola Greve (UFBA, Brazil), Luciana Arantes and Pierre Sens (INRIA, France)

Managing Business Health in the Presence of Malicious Attacks ................................................................. 9
Saman A. Zonouz, Aashish Sharma (University of Illinois, USA), HariGovind V. Ramasamy (IBM Research, USA), Zbigniew T. Kalbarczyk (University of Illinois, USA), Birgit Pfitzmann, Kevin McAuliffe (IBM Research, USA), Ravishankar K. Iyer, William H. Sanders (University of Illinois, USA) and Eric Cope (IBM Research, USA)

From Byzantine Fault Tolerance to Intrusion Tolerance (A Position Paper) ................................................. 15
Alysson Bessani (University of Lisboa, Portugal)
WRAITS Program

Session 2: Intrusion Detection and Response

Anomaly-Based Intrusion Detection in Software as a Service........19
Gustavo Nascimento (Portugal Telecom , Portugal) and Miguel Correia
(University of Lisboa, Portugal)

Combining Intrusion Detection and Recovery for Enhancing System
Dependability .................................................................25
Ajay Nagarajan, Quyen Nguyen, Robert Banks and Arun Sood (George Mason
University, USA)

A Cloud-Based Intrusion Detection and Response System for Mobile
Phones .................................................................31
Amir Houmansadr, Saman A. Zonouz and Robin Berthier (University of Illinois,
USA)

Session 3: Security Assessment

Continuous Mission-Oriented Assessment (CMA) of
Assurance.................................................................33
Patrick Hurley (Air Force Research Laboratory, USA), Partha Pal (BBN
Technologies, USA), Mathew Tan Creti (Purdue University, USA), and Amy Fedyk
(BBN Technologies, USA)

Guest Talk: Empirical Studies in Cybersecurity
Michel Cukier (Raytheon Company, USA)