Lecture Notes in Computer Science 11317

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

More information about this series at http://www.springer.com/series/7408

Issa Traore · Isaac Woungang
Sherif Saad Ahmed · Yasir Malik (Eds.)

Intelligent, Secure, and Dependable Systems in Distributed and Cloud Environments

Second International Conference, ISDDC 2018
Vancouver, BC, Canada, November 28–30, 2018
Proceedings

Springer

Editors
Issa Traore
University of Victoria
Victoria, BC, Canada

Isaac Woungang
Ryerson University
Toronto, ON, Canada

Sherif Saad Ahmed
University of Windsor
Windsor, ON, Canada

Yasir Malik
Concordia University of Edmonton
Edmonton, AB, Canada

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-030-03711-6 ISBN 978-3-030-03712-3 (eBook)
https://doi.org/10.1007/978-3-030-03712-3

Library of Congress Control Number: 2018960427

LNCS Sublibrary: SL2 – Programming and Software Engineering

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Welcome Message from ISDDC 2018 General Co-chairs

Welcome to the proceedings of the Second International Conference on Intelligent, Secure and Dependable Systems in Distributed and Cloud Environments (ISDDC 2018).

The past decade has witnessed tremendous advances in computing and networking technologies, with the appearance of new paradigms and the consolidation of existing ones. New paradigms such as the Internet of Things (IoT) and cloud computing and advances in mobile computation have disrupted how we live with, think of, interact with, and rely on computing technologies. Undoubtedly, the aforementioned technological advance helps improve many facets of human lives, for instance, through better health-care delivery, faster and more reliable communications, significant gains in productivity, and so on. At the same, it has raised significant challenges that we are still struggling to come to grips with effectively. Cybersecurity stands out as one of these areas that raise significant concerns about computing and networking technologies.

ISDDC is a conference series that provides a venue for researchers and practitioners to present, learn, and discuss recent advances in cybersecurity.

Every year, ISDDC receives several dozens of submissions from around the world. Building on the success from last year, ISDDC 2018 presented an exciting technical program that is the work of many volunteers. The program consisted of a combination technical papers, keynotes, and tutorials. The technical papers were peer reviewed by Program Committee (PC) members who are all cybersecurity experts and researchers, through a blind process.

We received a total of 28 papers this year, and accepted ten papers for inclusion in the proceedings and presentation at the conference, which corresponds to an acceptance rate of about 35%. Papers were reviewed by three PC members, in a single round of review.

ISDDC 2018 was also privileged to have select guest speakers to provide stimulating presentations on topics of wide interest. This year's distinguished speakers were:

- Dr. Baljeet Malhotra, Director of Research at Synopsys Inc., and Founder of TeejLab Inc.
- Mr. Deepak Rout, Executive Cybersecurity Advisor, Microsoft Inc.
- Mr. Mustapha Rachidi, Security Analyst, Bulletproof

We would like to thank all of the volunteers for their contributions to ISDDC 2018. Our thanks go to the authors, and our sincere gratitude goes to the Program Committee, who gave much extra time to carefully review the submissions.

We are pleased to announce selected papers will be invited to submit extended versions for publication in the Wiley journal *Security and Privacy*.

We would also like to thank the local organizing team, in particular Dean Irene Young and Ms. Lee Harris, from New York Institute of Technology, for their support and hard work in making this event a success. Our thanks go to our sponsors:

– New York Institute of Technology Vancouver Campus, for hosting ISDDC 2018
– Springer, for publishing the conference proceedings

Finally, we thank all the attendees and the larger ISDDC community for their continuing support, by submitting papers and by volunteering their time and talent in other ways.

We hope you will find the papers in the proceedings interesting.

Issa Traore
Isaac Woungang

Welcome Message from ISDDC 2018 Program Co-chairs

Welcome to the proceedings of the Second International Conference on Intelligent, Secure and Dependable Systems in Distributed and Cloud Environments (ISDDC 2018), which was held during November 28–30, at the New York Institute of Technology (NYIT), Vancouver, BC, Canada.

ISDDC provides a forum for cybersecurity researchers and practitioners from industry and government to meet and exchange ideas about progress and advances in the emerging areas of intelligent, secure, dependable systems and cloud environments.

The papers selected for publication in the proceedings of ISDDC 2018 span many research issues related to the design, analysis, implementation, management and control of dependable and secure systems, and covering aspects such as algorithms, architectures, and protocols dealing with network computing, ubiquitous and cloud systems, and Internet of Things systems. Operational security, intrusion detection, biometrics, cyber-threat intelligence, blockchain technology, access control and secure task offloading/storage in cloud computing, multiparty trust negotiation over distributed systems, to name a few, are examples of areas and applications of these contributed papers. We hope the participants of this conference will benefit from this coverage of a wide range of current hot-spot security-related topics.

In this edition, 28 papers were submitted, and peer-reviewed by the Program Committee members and external reviewers who are experts in the topical areas covered by the papers. The Program Committee accepted ten papers (about 35% acceptance ratio).

The conference program also included two distinguished keynote speeches and two tutorials.

Our thanks go to the many volunteers who contributed to the organization of ISDDC 2018. We would like to thank all authors for submitting their papers. We would also like to thank the Program Committee members for thoroughly reviewing the submissions and making valuable recommendations. We would like to thank the ISDDC 2018 local arrangements team for the excellent organization of the conference, and for their effective coordination creating the recipe for a very successful conference.

We hope you will enjoy the conference proceedings.

October 2018

Yasir Malik
Sherif Saad Ahmed

Organization

ISDCC 2018 Organizing Committee

General Co-chairs

Issa Traore	University of Victoria, Canada
Isaac Woungang	Ryerson University, Canada

Publicity Co-chairs

Isaac Woungang	Ryerson University, Canada
Watheq Elkarachi	Ain Shams University, Egypt

Program Co-chairs

Yasir Malik	Concordia University, Canada
Sherif Saad Ahmed	University of Windsor, Canada

Local Arrangements Chairs

Ahmed Awad	University of Washington, Bothell, USA
Tokunbo Makanju	New York Institute of Technology, Vancouver, Canada

Tutorial Chair

Ahmed Awad	University of Washington, Bothell, USA

Technical Program Committee

Petros Nicopolitidis	Aristotle University of Thessaloniki, Greece
Ilsun You	Soonchunhyang University, Republic of Korea
Wei Lu	Keene State College, USA
Sherali Zeadally	University of Kentucky, USA
Luca Caviglione	CNIT, Italy
Reza M. Parizi	New York Institute of Technology, Nanjing, China
Hamed Aly	Acadia University, Canada
Christine Chan	University of Regina, Canada
Enrico Schiavone	University of Florence, Italy
Rohit Ranchal	IBM Watson Health Cloud, USA
Danda B. Rawat	Howard University, USA

Marcelo Luis Brocardo	University of Santa Catarina, Brazil
Mohammad Derawi	Norwegian University of Science and Technology, Norway
Yudong Liu	Western Washington University, Bellingham, WA, USA
Babak Beheshti	New York Institute of Technology, New York, NY, USA
Wenjia Li	New York Institute of Technology, New York, NY, USA
Ahmed Mousaad	IBM Watson, USA
Ahmed Mostafa	Microsoft Amsterdam Area, The Netherlands
Watheq Elkarachi	Ain Shams University, Egypt
Isaac Woungang	Ryerson University, Canada
Issa Traore	University of Victoria, Canada
Sherif Saad Ahmed	University of Windsor, Canada
Yasir Malik	Concordia University of Edmonton, Canada
Ahmed Awad	University of Washington, Bothell, USA
Tokunbo Makanju	New York Institute of Technology, Vancouver, Canada
Amin Milani Fard	New York Institute of Technology, Vancouver, Canada
Wei Li	Northern Illinois University, DeKalb, USA

ISDDC 2018 Keynote Talks

Data-Driven Intelligence for Security Vulnerability Management at Scale

Baljeet Malhotra

Director of Research at Synopsys Inc., and Founder of TeejLab Inc.

Abstract. Monitoring publicly known security vulnerabilities in software systems is very important for enterprises. Organizations such as National Institute of Standards and Technology (NIST) regularly publish vulnerability reports (using Common Vulnerability Enumeration or CVE) to secure national IT networks and protect business interests at large. The main challenge in this context is that the software systems or tools against which the vulnerabilities are published are typically known differently to various stake holders that consume those vulnerable software systems. For instance, an organization may refer to one of its software components as my.program.js, however NIST may report a vulnerability on that particular software component as org_program.js according to their standards (using Common Platform Enumeration or CPE). Thousands of vulnerabilities are reported against millions of software components every year, which makes this problem very complex. In this talk, we'll discuss about a system that we built to match imprecise pieces of unstructured data to track vulnerabilities in software systems. The heart of the system is Natural Language Processing techniques that are capable of searching vulnerabilities from large volumes of unstructured data regardless of how the software systems are named. We'll conclude with a view on data-driven intelligence that can address the scalability and volume issues faced by commercial vulnerability management solutions.

Incident Management: Investigating a Malware

Mustapha Rachidi

Security Analyst at Bulletproof, Fredericton, New Brunswick

Abstract. Security Analyst is a challenging role in performing a good investigation of all security incidents that occur. On that account, the role demands continuous monitoring to make sure the environment is always healthy and secure. For that reason, Security Analysts use lots of tools and technologies like Security Information and Event Management (SIEM) that provides real-time analysis of security logs and events generated by applications and network appliances. A good resolution of any incident requires us to have an incident management process put in place with well defined procedures that detail the appropriate responses to incidents. The objective of having such a process is to restore the operations back to normal when an incident occurs while minimizing the risk by limiting the incident impact. In this presentation, the different phases of an incident management process will be explained from a security analyst perspective. Then, in this presentation, a real application for the incident management process will be discussed: a malware that has been detected will be investigated while following the process of the incident response management that is used by the SOC to mitigate the impact, analyze the malware and make the necessary response to restore the operations to normal.

Cyber Resiliency in the Era of Cloud, Mobility and Big Data

Deepak Rout

Executive Security Advisor, Microsoft Canada

Abstract. Digital transformation is revolutionizing our world. Cloud computing, Social Media, and Mobile technologies have re-modelled our world, and are being further reshaped at a rapid pace by Artificial Intelligence and Machine Learning paradigms. This has created an unprecedented impact globally across both enterprises and consumers, posing significant risks that needs to be acknowledged and managed. It is important to know how your business or organization is impacted by cyber resiliency and further, how you can help your business addressing such issue. Partnership with organizations with unique insights into cloud, mobility and artificial intelligence may go a long way in this regard. The objective of this talk is to share some light on how to deal with the issue of cyber resiliency in this Era of cloud, mobility and Bigdata.

ISDDC 2018 Tutorials

Attack Graphs in Cybersecurity – Evolution and Practice

Paulo Quinan

University of Victoria, ECE Department, Victoria, BC, Canada

Abstract. Attack Graphs are very powerful tools used in many areas of information security including threat modelling, intrusion detection and prevention and forensic analysis given their capabilities in helping security analysts identify how attackers can exploit, or have exploited, vulnerabilities in a system in order to compromise it. Traditionally, attack graphs were generated manually, however that is an error prone process that gets exponentially harder the more elements or nodes are added to the system being analyzed. To overcome this issue many automatic generation tools and techniques have been proposed, and while those tools have allowed the generation of attack graphs of very large and complex systems, they have also made the analysis of the resulting attack graphs ever more complex. That is compounded by the ever growing number of attack graph variations, each aiming to elucidate different aspects of the security issues faced by the system. Together, the complexity and the large number of variations used in the industry, mean that learning to generate and analyze attack graphs can be a daunting task even for experienced security analysts. This tutorial aims to help those wishing to start learning about attack graphs by presenting an introductory overview of the subject. We will discuss how and when to use them, some of their most common types, like the state attack graph, the logical attack graph, the privilege graph and the vulnerability graph, the different tools and techniques used to generate them, and some of the most important open challenges in the field.

Engineering Location Privacy Attacks in VANETs

Ikjot Saini

School of Computer Science, University of Windsor, Windsor, ON, Canada

Abstract. Vehicular Ad-hoc Networks (VANET) are envisioned as an integral part of Intelligent Transportation Systems. However, the security and privacy risks associated with the wireless communication are often overlooked. In fact, messages exchanged in VANET wireless communication carries personally identifiable information. This introduces several privacy threats that could limit the adaptation of VANET.PREXT is a unified and extensible framework that simulate pseudonym change schemes (i.e. privacy schemes) in VANET. It supports seven privacy schemes of different approaches including silent period, context-based and mix-zone and can be easily extended to include more schemes. It includes adversary modules that can eavesdrop vehicle messages and track their movements. This adversary is used in measuring the gained privacy in terms of several popular metrics such as entropy, traceability, and pseudonym usage statistics. In this short Tutorial, we will demonstrate how location privacy attacks could be designed, implemented and analyzed using PREXT and other VANETs simulations tools.

Static Analysis in Fileless Cryptocurrency-mining Malware

Liu Meijia

AV Analyst, Fortinet Inc., Vancouver, BC, Canada

Abstract. Fileless Malware attacks became dramatically increasing since 2016. It is well known that antivirus software is designed to scan computers by malware signatures and block thesemalware from executing. Unlike traditional malware intends to trick people to download files or exploit software flaw to install files for delivering payload, fileless malware executes malicious code directly from memory rather than installing any software on a target machine. Since there are no malware files on the hard disk, it is more difficult to detect. The mining fileless malware that this tutorial provided utilize legitimate software tools like Windows Management Instrumentation (WMI) and PowerShell to infect machines by obfuscated script. The PowerShell script is executed to communicate with C&C server and update to the latest version. By Mimikatz tool, the user account details from the infected machine are obtained in the process. It can propagate itself via WMI and EternalBlue, and place itself into remote computer WMI database. Furthermore, it exploits vulnerabilities in MS16-032, MS15-051 and CVE-2018-8120 to escalate user privileges depending on 32-bit and 64-bit operating system. At last, it uses WMI as persistence mechanism to launch miner with the reflective PE injection about every 93.3 minutes. Finally, the tutorial is offering some countermeasures to avoid this kind of attack. According to today's threat in cybersecurity, scanning the hard drive for malicious files is not enough for antivirus team. Looking for evidence in memory becomes indispensable part during antivirus work.

Contents