

SpringerBriefs in Cybersecurity

Editor-in-Chief

Sandro Gaycken, Digital Society Institute, European School of Management and Technology (ESMT), Stuttgart, Baden-Württemberg, Germany

Series editors

Sylvia Kierkegaard, International Association of IT Lawyers, Highfield, Southampton, UK

John Mallery, Computer Science and Artificial Intelligence, Massachusetts Institute of Technology, Cambridge, MA, USA

Steven J. Murdoch, University College London, London, UK

Kenneth Geers, Taras Shevchenko University, Kyiv, Kiev's'ka, Ukraine

Michael Kasper, Department of Cyber-Physical Systems Security, Fraunhofer Institute SIT, Darmstadt, Hessen, Germany

Cybersecurity is a difficult and complex field. The technical, political and legal questions surrounding it are complicated, often stretching a spectrum of diverse technologies, varying legal bodies, different political ideas and responsibilities. Cybersecurity is intrinsically interdisciplinary, and most activities in one field immediately affect the others. Technologies and techniques, strategies and tactics, motives and ideologies, rules and laws, institutions and industries, power and money—all of these topics have a role to play in cybersecurity, and all of these are tightly interwoven.

The *SpringerBriefs in Cybersecurity* series is comprised of two types of briefs: topic- and country-specific briefs. Topic-specific briefs strive to provide a comprehensive coverage of the whole range of topics surrounding cybersecurity, combining whenever possible legal, ethical, social, political and technical issues. Authors with diverse backgrounds explain their motivation, their mindset, and their approach to the topic, to illuminate its theoretical foundations, the practical nuts and bolts and its past, present and future. Country-specific briefs cover national perceptions and strategies, with officials and national authorities explaining the background, the leading thoughts and interests behind the official statements, to foster a more informed international dialogue.

More information about this series at <http://www.springer.com/series/10634>

Aamo Iorliam

Cybersecurity in Nigeria

A Case Study of Surveillance and Prevention
of Digital Crime

 Springer

Aamo Iorliam
Department of Mathematics
and Computer Science
Benue State University
Makurdi, Nigeria

ISSN 2193-973X

ISSN 2193-9748 (electronic)

SpringerBriefs in Cybersecurity

ISBN 978-3-030-15209-3

ISBN 978-3-030-15210-9 (eBook)

<https://doi.org/10.1007/978-3-030-15210-9>

Library of Congress Control Number: 2019933714

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2019

This work is subject to copyright. All rights are solely and exclusively licensed by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, express or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

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

To God Almighty

Foreword

This five-chapter book titled *Cybersecurity in Nigeria—A Case Study of Surveillance and Prevention of Digital Crime* by Dr. Iorliam is a handbook containing all you need to know about cyber surveillance in Nigeria. It looks at how cyber surveillance could stop digital crimes in Nigeria and by extension the world.

The author knows his stuff, having earned an M.Sc. in Forensic Computing with a distinction from Coventry University and a Ph.D. in Computer Science with a thesis focusing on the Application of Power Laws to Biometrics, Forensics and Network Traffic Analysis from the University of Surrey, both in UK. From these universities, he was able to sharpen and cut his academic teeth.

The book demonstrates his knowledge of his research areas which include Power laws, machine learning, data mining, image analysis, digital and multimedia forensics, cybersecurity, biometrics, computer forensics and network traffic analysis.

From his research standpoint, the author delved into areas of the application of forensic science to solve problems in network traffic analysis, fake news detection and the development of a digital surveillance software to prevent/detect digitally facilitated crimes in Nigeria.

This book is divided into five chapters;

Chapter 1 provides the necessary introduction that a reader needs to be able to understand and get the best out of the book.

Chapter 2 shows how Natural laws can effectively detect malicious traffic on the Internet.

Chapter 3 shows how Natural laws can solve a very important challenge in Nigeria—fake news detection.

Chapter 4 provides an explanation to how cyber crimes occur in Nigeria and the need for cybersecurity and mobile device forensics to solve this challenge.

Chapter 5 proposes a digital surveillance software (A-BOT) that can effectively stop digital crimes in Nigeria.

This book is a must read for forensic scientists, cryptographers, stenographers and all law enforcement agencies in Nigeria. It is a gift from Dr. Iorliam to a world in dire need of the knowledge on the secrets of forensic science in solving different types of crimes. I strongly recommend this book to you!

Lokoja, Nigeria
January 2019

Prof. Sunday Eric Adewumi, Ph.D., fncs
Dean, Faculty of Science
Federal University Lokoja

Preface

It is not new that the Nigerian cyber space and its cyber infrastructure is very porous and has given much room to cyber attackers to freely operate. In 2017, 3500 cyber attacks on the Nigerian cyber space were successful. This led to Nigeria losing 450 million dollars [1].

These cyber crimes are hampering Nigeria's digital economy. This further explains why many Nigerians are not convinced about Internet marketing and online transactions that involve money. This is worrisome even for the Nigerian military intelligence. If sensitive conversations using digital devices (e.g. phones or computers) are not well monitored, then Nigeria will be defeated in the cyber warfare. If Nigeria loses the cyber warfare, then our digital economy, military intelligence and related sensitive firms will also crumble.

The Nigerian Army Cyber Warfare Command was instituted in 2018 with a task to solve terrorism, banditry and other attacks by criminal groups in Nigeria [2]. This is a right step by the Nigerian government. However, there is every need to provide digital surveillance to the Nigerian cyber space to assist law enforcement agencies in Nigeria to prevent/detect these digitally facilitated crimes.

Therefore, monitoring of Nigeria's cyber space and its cyber infrastructure has become imperative given that the rate of criminal activities has increased tremendously using technology. Cyber infrastructure consists of computing systems, data storage systems, advanced instruments and data repositories, visualization environments and people, all linked by high-speed networks to make possible scholarly innovation and discoveries not otherwise possible. Information technology systems that provide particularly powerful and advanced capabilities could also be referred to as cyber infrastructure [3]. This book proposes the use of digital surveillance aimed at investigating, detecting, uncovering and interpreting any fraud associated with the cyber space and critical cyber infrastructures in Nigeria. This will make the Nigerian digital ecosystem free of cyber attackers. This digital surveillance includes

passive forensic investigations (investigations where an attack has already occurred) and active forensic investigations (real-time investigations to track attackers). Hence, producing a zero-cyber crime Nigeria.

Makurdi, Nigeria
January 2019

Dr. Aamo Iorliam

References

1. The Paradigm (2017) Nigerias cyberspace has become very porous-senate. <http://www.theparadigmng.com/2017/05/24/nigerias-cyberspace-become-porous-senate/>. Accessed 27 Nov 2018
2. Sunnewsonline (2018) Insurgency: army establishes cyber warfare command. <http://sunnewsonline.com/insurgency-army-establishes-cyber-warfare-command/>. Accessed 27 Nov 2018
3. Indiana University (2018) What is cyberinfrastructure?. <https://kb.iu.edu/d/auhf>. Accessed 27 Nov 2018

Acknowledgements

Special thanks to the following:

- Springer Team: For your support towards making the publication of this book a huge success.
- My Ph.D. supervisors: Prof. Anthony T. S. Ho, Prof. Shujun Li, Dr. Norman Poh and Prof. Adrian Waller who mentored me.
- To my friends: Dr. Santosh Tirunagari, Shangbum Caleb Faveren, Dr. Nyinoh Iveren, Oshido Barnabas, Ode Egena, Dr. Ikyanyon Darius.
- To my family members: Mr. and Mrs. Iorliam (Dad and Mum), Eng. Dr. and Dr. (Mrs.) Yala Iorliam, Pastor and Mrs. Aondowase Tsuaa, Mr. and Barr. (Mrs.) Nguetar Iorliam, Mr. and Mrs. Ukaan.

And most importantly, my wife Iveren (Udookwase), and my two daughters, Afam and Asoose, who supported and encouraged me throughout the whole process of writing this book.

Contents

1	Introduction	1
1.1	Main Contributions	1
1.2	Document Structure	2
2	Natural Laws (Benford’s Law and Zipf’s Law) for Network Traffic Analysis	3
2.1	Contribution	4
2.2	Benford’s Law	4
2.3	Zipf’s Law	6
2.4	Network Traffic Analysis and IDS	6
2.4.1	Flow-Based IDS	7
2.5	Network Flows and TCP Flows	8
2.6	Application to Network Traffic Analysis	9
2.6.1	Method Description	9
2.6.2	The Metrics	9
2.6.3	Analysis of Different Flow Ordering Options	10
2.7	Experimental Setup and Results	11
2.7.1	Datasets Used for Our Experiments	11
2.7.2	Flow Size or Flow Size Difference	12
2.7.3	How to Determine Flow Window Size	12
2.7.4	TCP Flow Ordering	13
2.7.5	More Results on Different Datasets	13
2.7.6	Zipf’s Law for Network Traffic Analysis	14
2.7.7	Zipf’s Law for Malicious, Non-malicious, Mixture of Malicious and Non-malicious Network Traffic	16
2.7.8	Comparative Analysis of Zipf’s Law and Benford’s Law with Implications	17
2.8	Conclusion	20
	References	20

- 3 Combination of Natural Laws (Benford’s Law and Zipf’s Law) for Fake News Detection 23**
 - 3.1 Combination of Benford’s Law and Zipf’s Law for Fake News Detection 24
 - 3.2 Results and Discussions 29
 - 3.3 Conclusion 29
 - References 30

- 4 Cybersecurity and Mobile Device Forensic 31**
 - 4.1 Nigeria and Internet Fraud 32
 - 4.2 Reasons for Increase in Cyber Crimes in Nigeria 34
 - 4.3 Types of Cyber Crimes in Nigeria 35
 - 4.4 Link Between Mobile Device Forensics and Cybersecurity 37
 - 4.5 Cybersecurity Laws and Punishment in Nigeria 40
 - 4.6 Conclusion 42
 - References 43

- 5 Proposed Digital Surveillance Software 45**
 - 5.1 Introduction 45
 - 5.2 System Analysis and Design 49
 - 5.3 Product Features and How It Works 49
 - 5.4 The Solution (A-BOT) 52
 - 5.5 Advantages of the Proposed System 54
 - 5.6 Conclusion 55
 - References 55