Automatic Defense against Zero-day Polymorphic Worms in Communication Networks

Authors: Mohssen Mohammed and Al-Sakib Khan Pathan

Dedicated to …

To my father Mohammed Zain Elabdeen Mohammed; my sister Maali Mohammed Zian Elaabdeen, Faculty of Mathematical Science, University of Khartoum - Khartoum-Sudan, especially I would like to thank Dr. Mohsin Hashim, and Dr. Eihab Bashier. Dr. Lorenzo Cavallaro, Information Security Group, Royal Holloway, University of London.

- Mohssen Mohammed

To my father Abdus Salam Khan Pathan, my mother Delowara Khanom, and my loving wife Labiba Mahmud.

- Al-Sakib Khan Pathan

Automatic Defense against Zero-day Polymorphic Worms in Communication Networks

Preface

Internet worms pose a major threat to Internet infrastructure security, and their destruction is truly costly. Computer Worm is a kind of malicious program that self-replicates automatically within a computer network. Worms are in general, a serious threat to computers connected to the Internet and its proper functioning. These malicious programs can spread by exploiting low-level software defects, and can use their victims for illegitimate activities; such as corrupting data, sending unsolicited electronic mail messages, generating traffic for distributed Denial of Service (DoS) attacks, or stealing information. Today, the speed at which the worm propagates poses a serious security threat to the Internet.

Polymorphic worm is a kind of worm that is able to change its payload in every infection attempt, so it can evade the Intrusion Detection Systems (IDSs), and damage data, delay the network, cause information theft, and other illegal activities that lead to even for example, high financial loss. To defend the network against the worm, intrusion detection systems (IDSs) such as Bro and Snort are commonly deployed at the edge of network and the Internet. The main principle of these IDSs is to analyze the traffic to compare it against the signatures stored in their databases. Whenever a novel worm is detected in the Internet, the common approach is that the experts from security community analyze the worm code manually and produce a signature. The signature is then distributed and each IDS updates its database with this new signature.

This approach of creating signature is human intensive, very slow and when we have threats of very fast replicating worms (that take as small as few seconds to bring down the entire network) like Zero-day polymorphic worms, the need of an alternative is recognized. The alternative approach is to find a way to automatically generate signatures that are relatively faster to generate and are of acceptable good quality. This book focuses on how we can automatically generate signatures for unknown polymorphic worms.

Usually, to know how to automatically generate signatures for polymorphic worm attacks, reading a good number of books and information sources is necessary. To really understand the subject matter, a reader usually needs to read a wide range of books, like:

a) **Books about Computer Networking**
   - To generate signatures for polymorphic worms, a strong background in the computer networking is needed. Especially, the knowledge is needed about the network topologies, network routing protocols, network IP addresses, and other network related mechanisms.

b) **Books about Network Security**

- Such books give general information about how to secure the communications in the network. Worm tackling may come as a part of such a book but concrete information about unknown or Zero-day worm may be missing.

c) Books about Intrusion Detection Systems (IDSs)

- Such books give information about how the IDSs work, what are the types of IDSs, what are the types of signatures that are used in the IDSs, etc.

d) Books about Intrusion Prevention Systems (IPSs)

- These types of books can give information about how the IPSs work and we can know what the differences are between the IDSs and IPSs, and so on.

e) Books about Honeypot

- Such books give information about what is the Honeypot, where we can use it, what is the importance of Honeypot, how we can collect polymorphic worms using it, etc.

f) Books about polymorphic worms

- These books provide information about the polymorphic worm attacks, how the polymorphic worms change their payloads, how they are launched in the Internet, etc.

g) Books about String Matching Algorithm

h) Books about Statistical method

i) Books about Artificial Intelligent Systems

j) Books about Machine Learning

To generate signatures for polymorphic worm attacks, we need some kinds of algorithms. So, all these books of categories: (g), (h), (i), and (j) can help find suitable algorithms that we can use to generate good signatures for polymorphic worms.

To know, find, and read all these books or documents are a very time consuming and difficult task. Our own experience shows that it really needs considerable efforts to reach even up to a minimum level to understand the functions of worms and then tackling them when they are polymorphic and unknown. Hence, keeping this personal experience in mind, the objective of our book is to combine all the knowledge of these sources in a single volume.

This is not a thick book considering number of pages, but we have written it in a reasonable manner to address all the critical issues regarding the topic. We have included the core information and tried to explain exactly what is needed to automatically generate signatures for unknown polymorphic worms. We hope that our book will fill the existing void in the field of automatic handling of Zero-day polymorphic worms.

The target audiences of this book are the researchers, post-graduate students, industry experts, and academics who are working on malware detection in communication networks, especially polymorphic worm detection. We hope that this book will reduce the time for the practitioners and students in searching information for doing research in this area. It will directly provide valuable information in a single volume for their convenience.

So, this book is expected to be very useful in terms of saving time and money. For the benefit of the readers, we have included the latest information along with future views and visions so that the information could be used for several years afterwards. As some fundamental data and practical information are combined for the general readers, we hope it will also serve the purpose of providing general information about worms which would not wear out for a long time in the future.

To emphasize the danger of polymorphic worms, it should noted that they can create serious problems for the Internet security as they can be used to incur delay in a network, steal information, delete information, launch flooding attacks against servers, and so on. Polymorphic worm attacks are considered as one of the top attacks in the globe against the Internet security and their destruction is often extremely costly (or, nearly impossible). We have extensively surveyed the currently available books and documents in the relevant areas. Our finding shows that currently there is no suitable alternative to this book. There are some network security related books which have some or very less information on the topic as small parts but they are not sufficient. So, we have taken this initiative to make things easier for the researchers and common readers. We should add the point that the book requires some knowledge on the topic to understand in depth, otherwise the preliminary chapters would be easily accessible for any reader of the area.

Before ending the preface of this book, we must give thanks to the Almighty, who gave us time to complete this work and kept us fit for work throughout the working period. Special thanks must be given to our family members who supported us to work till late nights on many occasions. Special thanks to ***Richard O'Hanley*** for his kind support throughout the development period of the book. Last but not the least; we would like to thank the publication staffs for their prompt replies to various queries and cordial cooperation.

Best Wishes,
The Authors

Mohssen Mohammed, Ph.D.
University of Bahri
Khartoum, Sudan
Email: m_zin44@hotmail.com

Al-Sakib Khan Pathan, Ph.D.
International Islamic University Malaysia
Jalan Gombak 53100, Kuala Lumpur, Malaysia
Email: sakib@iium.edu.my , sakib.pathan@gmail.com

BIOGRAPHIES of the AUTHORS

Mohssen Mohammed received his B.Sc. (Honors) degree in Computer Science from Computer Man College for Computer Studies (Future University), Khartoum – Sudan in 2003. In 2006, received the M.Sc. degree in Computer Science from the Faculty of Mathematical Sciences – University of Khartoum, Sudan. In 2012 received Ph.D. degree in Electrical Engineering from Cape Town University, South Africa. He published several papers at top international conferences such as GLOBECOM and MILCOM. He has served as a Technical Program Committee member in numerous international conferences like ICSEA 2010, ICNS 2011. He got University of Cape Town prize for International Scholarship for Academic Merit (Years 2007, 2008, and 2009). From 2005 to 2012 he has been working as a permanent academic staff at the University of Juba, South of Sudan. Now he is working as Assistant Professor in the College of Computer Science & Information Technology, Bahri University, Khartoum Sudan. His research interest includes Network Security, especially Intrusion detection and prevention systems, Honeypots, Firewalls, and Malware Detection Methods.

Al-Sakib Khan Pathan received Ph.D. degree in Computer Engineering in 2009 from Kyung Hee University, South Korea. He received B.Sc. degree in Computer Science and Information Technology from Islamic University of Technology (IUT), Bangladesh in 2003. He is currently an Assistant Professor at Computer Science department in International Islamic University Malaysia (IIUM), Malaysia. Till June 2010, he served as an Assistant Professor at Computer Science and Engineering department in BRAC University, Bangladesh. Prior to holding this position, he worked as a Researcher at Networking Lab, Kyung Hee University, South Korea till August 2009. His research interest includes wireless sensor networks, network security, and e-services technologies. He is a recipient of several awards/best paper awards and has several publications in these areas. He has served as a Chair, Organizing Committee Member, and Technical Program Committee member in numerous international conferences/workshops like HPCS, ICA3PP, IWCMC, VTC, HPCC, IDCS, etc. He is currently serving as the Editor-in-Chief of IJIDCS, an Area Editor of IJCNIS, Editor of IJCSE, Inderscience, Associate Editor of IASTED/ACTA Press IJCA and CCS, Guest Editor of some special issues of top-ranked journals, and Editor/Author of five published books. He also serves as a referee of some renowned journals. He is a member of Institute of Electrical and Electronics Engineers (IEEE), USA; IEEE Communications Society (IEEE ComSoc), USA, and IEEE ComSoc Bangladesh Chapter, and several other international organizations.