



Automatic Defense Against Zero-day Polymorphic Worms in Communication Networks

By Mohssen Mohammed, Al-Sakib Khan Pathan

Download now

Read Online 

Automatic Defense Against Zero-day Polymorphic Worms in Communication Networks By Mohssen Mohammed, Al-Sakib Khan Pathan

Able to propagate quickly and change their payload with each infection, polymorphic worms have been able to evade even the most advanced intrusion detection systems (IDS). And, because zero-day worms require only seconds to launch flooding attacks on your servers, using traditional methods such as manually creating and storing signatures to defend against these threats is just too slow.

Bringing together critical knowledge and research on the subject, **Automatic Defense Against Zero-day Polymorphic Worms in Communication Networks** details a new approach for generating automated signatures for unknown polymorphic worms. It presents experimental results on a new method for polymorphic worm detection and examines experimental implementation of signature-generation algorithms and double-honeynet systems.

If you need some background, the book includes an overview of the fundamental terms and concepts in network security, including the various security models. Clearing up the misconceptions about the value of honeypots, it explains how they can be useful in securing your networks, and identifies open-source tools you can use to create your own honeypot. There's also a chapter with references to helpful reading resources on automated signature generation systems.

The authors describe cutting-edge attack detection approaches and detail new algorithms to help you generate your own automated signatures for polymorphic worms. Explaining how to test the quality of your generated signatures, the text will help you develop the understanding required to effectively protect your communication networks. Coverage includes intrusion detection and prevention systems (IDPS), zero-day polymorphic worm collection methods, double-honeynet system configurations, and the implementation of double-honeynet architectures.

 [Download Automatic Defense Against Zero-day Polymorphic Wor
...pdf](#)

 [Read Online Automatic Defense Against Zero-day Polymorphic W
...pdf](#)

Automatic Defense Against Zero-day Polymorphic Worms in Communication Networks

By Mohssen Mohammed, Al-Sakib Khan Pathan

Automatic Defense Against Zero-day Polymorphic Worms in Communication Networks By Mohssen Mohammed, Al-Sakib Khan Pathan

Able to propagate quickly and change their payload with each infection, polymorphic worms have been able to evade even the most advanced intrusion detection systems (IDS). And, because zero-day worms require only seconds to launch flooding attacks on your servers, using traditional methods such as manually creating and storing signatures to defend against these threats is just too slow.

Bringing together critical knowledge and research on the subject, **Automatic Defense Against Zero-day Polymorphic Worms in Communication Networks** details a new approach for generating automated signatures for unknown polymorphic worms. It presents experimental results on a new method for polymorphic worm detection and examines experimental implementation of signature-generation algorithms and double-honeynet systems.

If you need some background, the book includes an overview of the fundamental terms and concepts in network security, including the various security models. Clearing up the misconceptions about the value of honeypots, it explains how they can be useful in securing your networks, and identifies open-source tools you can use to create your own honeypot. There's also a chapter with references to helpful reading resources on automated signature generation systems.

The authors describe cutting-edge attack detection approaches and detail new algorithms to help you generate your own automated signatures for polymorphic worms. Explaining how to test the quality of your generated signatures, the text will help you develop the understanding required to effectively protect your communication networks. Coverage includes intrusion detection and prevention systems (IDPS), zero-day polymorphic worm collection methods, double-honeynet system configurations, and the implementation of double-honeynet architectures.

Automatic Defense Against Zero-day Polymorphic Worms in Communication Networks By Mohssen Mohammed, Al-Sakib Khan Pathan **Bibliography**

- Sales Rank: #6064295 in Books
- Brand: Brand: Auerbach Publications
- Published on: 2013-05-21
- Original language: English
- Number of items: 1
- Dimensions: 9.30" h x .90" w x 6.20" l, .0 pounds
- Binding: Hardcover
- 337 pages

 [Download Automatic Defense Against Zero-day Polymorphic Wor ...pdf](#)

 [Read Online Automatic Defense Against Zero-day Polymorphic W ...pdf](#)

Download and Read Free Online Automatic Defense Against Zero-day Polymorphic Worms in Communication Networks By Mohssen Mohammed, Al-Sakib Khan Pathan

Editorial Review

About the Author

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 his 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.

Users Review

From reader reviews:

Joseph Tucker:

Book is usually written, printed, or highlighted for everything. You can know everything you want by a guide. Book has a different type. As you may know that book is important point to bring us around the world. Alongside that you can your reading ability was fluently. A book Automatic Defense Against Zero-day Polymorphic Worms in Communication Networks will make you to always be smarter. You can feel far more confidence if you can know about almost everything. But some of you think that open or reading the book make you bored. It isn't make you fun. Why they may be thought like that? Have you seeking best book

or suitable book with you?

Agustin Byler:

Information is provisions for those to get better life, information today can get by anyone from everywhere. The information can be a understanding or any news even a concern. What people must be consider when those information which is inside former life are challenging to be find than now is taking seriously which one is appropriate to believe or which one the particular resource are convinced. If you receive the unstable resource then you get it as your main information there will be huge disadvantage for you. All those possibilities will not happen inside you if you take Automatic Defense Against Zero-day Polymorphic Worms in Communication Networks as your daily resource information.

Sandra Kelley:

The particular book Automatic Defense Against Zero-day Polymorphic Worms in Communication Networks will bring that you the new experience of reading the book. The author style to elucidate the idea is very unique. In case you try to find new book you just read, this book very suitable to you. The book Automatic Defense Against Zero-day Polymorphic Worms in Communication Networks is much recommended to you to study. You can also get the e-book from the official web site, so you can easier to read the book.

Arthur Freeman:

Within this era which is the greater man or woman or who has ability to do something more are more important than other. Do you want to become certainly one of it? It is just simple solution to have that. What you have to do is just spending your time little but quite enough to possess a look at some books. One of many books in the top checklist in your reading list is Automatic Defense Against Zero-day Polymorphic Worms in Communication Networks. This book that is qualified as The Hungry Mountains can get you closer in turning out to be precious person. By looking upward and review this e-book you can get many advantages.

Download and Read Online Automatic Defense Against Zero-day Polymorphic Worms in Communication Networks By Mohssen Mohammed, Al-Sakib Khan Pathan #Z1J4QSAD5VU

Read Automatic Defense Against Zero-day Polymorphic Worms in Communication Networks By Mohssen Mohammed, Al-Sakib Khan Pathan for online ebook

Automatic Defense Against Zero-day Polymorphic Worms in Communication Networks By Mohssen Mohammed, Al-Sakib Khan Pathan Free PDF d0wnl0ad, audio books, books to read, good books to read, cheap books, good books, online books, books online, book reviews epub, read books online, books to read online, online library, greatbooks to read, PDF best books to read, top books to read Automatic Defense Against Zero-day Polymorphic Worms in Communication Networks By Mohssen Mohammed, Al-Sakib Khan Pathan books to read online.

Online Automatic Defense Against Zero-day Polymorphic Worms in Communication Networks By Mohssen Mohammed, Al-Sakib Khan Pathan ebook PDF download

Automatic Defense Against Zero-day Polymorphic Worms in Communication Networks By Mohssen Mohammed, Al-Sakib Khan Pathan Doc

Automatic Defense Against Zero-day Polymorphic Worms in Communication Networks By Mohssen Mohammed, Al-Sakib Khan Pathan Mobipocket

Automatic Defense Against Zero-day Polymorphic Worms in Communication Networks By Mohssen Mohammed, Al-Sakib Khan Pathan EPub

Z1J4QSAD5VU: Automatic Defense Against Zero-day Polymorphic Worms in Communication Networks By Mohssen Mohammed, Al-Sakib Khan Pathan