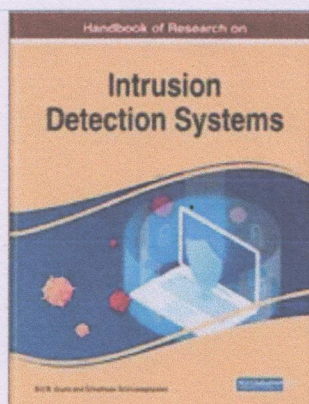


10% Discount on All E-Books through IGI Global's Online Bookstore Extended

(10% discount on all e-books cannot be combined with most offers. Discount is valid on purchases made directly through IGI Global Online Bookstore (www.igi-global.com) (<https://www.igi-global.com/>) and may not be utilized by booksellers and distributors. Offer does not apply to e-Collections and exclusions of select titles may apply. Offer expires December 31, 2022.)

[Browse Titles \(https://www.igi-global.com/search/?p=&ctid=1\)](https://www.igi-global.com/search/?p=&ctid=1)



A Survey on Detection and Analysis of Cyber Security Threats Through Monitoring Tools

Manjunath Kotari (Alva's Institute of Engineering and Technology, Moodbidri, India) and Niranjan N. Chiplunkar (NMAM Institute of Technology, Nitte, India)

Source Title: Handbook of Research on Intrusion Detection Systems (/book/handbook-research-intrusion-detection-systems/235719)

Copyright: © 2020

Pages: 28

DOI: 10.4018/978-1-7998-2242-4.ch005

OnDemand PDF
Download:

\$37.50

() Available

[Current Special Offers](#)

Abstract

Cyber crime is a serious threat for day-to-day transactions of the digital life. Overexposure of the personal details in social networks will lead to the cyber crime case. Therefore, detection and monitoring of cyber crime are challenging tasks. The cyber criminals are continually flooding the various intrusions all over the network. The cyber safety team should have a noteworthy challenge of filtering various such information. Continuous nonstop cyberattacks or intrusion examinations by security tools will significantly improve the threat alerts. However, cyber security becomes more expensive in the case of the above methods. The chapter provides systematic survey of various cyber security threats, evolution of intrusion detection systems, various monitoring mechanisms, open source cyber security monitoring tools, and various assessment techniques. The chapter also proposes a model of Cyber security detection and monitoring system and its challenges.

Chapter Preview

1. Introduction

Cyber security threats are major hurdle for the development activities of the Information Technology (IT) industry. The IT industry is facing severe crisis of cyber-crime activities in their business. A large set of data and assets of organizations are placed in cloud-based platform. The virtual cloud computing is facing various threats which include, Intrusions, Malwares, and Mining of Crypto currency. The Virtual Machines faces intrusions and impersonations in the cloud environments. The bitcoin attracts more


PRINCIPAL

Alva's Institute of Engg. & Technology,
Moodbidri, Karnataka, India

Top

Table of Contents

Preface	xix
Acknowledgment	xxiii
Chapter 1	
Intelligent User Profiling Based on Sensors and Location Data to Detect Intrusions on Mobile Devices.....	1
<i>Pedro Miguel Sánchez Sánchez, Universidad de Murcia, Spain</i> <i>José María Jorquera Valero, Universidad de Murcia, Spain</i> <i>Alberto Huertas Celdran, Waterford Institute of Technology, Ireland</i> <i>Gregorio Martínez Pérez, Universidad de Murcia, Spain</i>	
Chapter 2	
Improved Transmission of Data and Information in Intrusion Detection Environments Using the CBEDE Methodology	26
<i>Reinaldo Padilha França, State University of Campinas (UNICAMP), Brazil</i> <i>Yuzo Iano, State University of Campinas (UNICAMP), Brazil</i> <i>Ana Carolina Borges Monteiro, State University of Campinas (UNICAMP), Brazil</i> <i>Rangel Arthur, State University of Campinas (UNICAMP), Brazil</i>	
Chapter 3	
Machine Learning Techniques for Intrusion Detection	47
<i>Tameem Ahmad, Department of Computer Engineering, Z. H. College of Engineering and Technology, Aligarh Muslim University, Aligarh, India</i> <i>Mohd Asad Anwar, Department of Computer Engineering, Z. H. College of Engineering and Technology, Aligarh Muslim University, Aligarh, India</i> <i>Misbahul Haque, Department of Computer Engineering, Z. H. College of Engineering and Technology, Aligarh Muslim University, Aligarh, India</i>	
Chapter 4	
Network Attack Detection With SNMP-MIB Using Deep Neural Network	66
<i>Mouhammd Sharari Alkasassbeh, Computer Science Department, Princess Sumaya University for Technology, Jordan</i> <i>Mohannad Zead Khairallah, Computer Science Department, Princess Sumaya University for Technology, Jordan</i>	


PRINCIPAL
 Aligarh Institute of Engg. & Technology,
 Aligarh, MOODBIDRI - 574 225, D.K.

Chapter 5

A Survey on Detection and Analysis of Cyber Security Threats Through Monitoring Tools.....	77
--	----

Manjunath Kotari, Alva's Institute of Engineering and Technology, Moodbidri, India

Niranjan N. Chiplunkar, NMAM Institute of Technology, Nitte, India

Chapter 6

Identification and Classification of Cyber Threats Through SSH Honeypot Systems.....	105
--	-----

*José María Jorquera Valero, Department of Information and Communications Engineering,
University of Murcia, Spain*

*Manuel Gil Pérez, Department of Information and Communications Engineering, University
of Murcia, Spain*

*Alberto Huertas Celdrán, Telecommunications Software and Systems Group, Waterford
Institute of Technology, Ireland*

*Gregorio Martínez Pérez, Department of Information and Communications Engineering,
University of Murcia, Spain*

Chapter 7

Data Access Management System in Azure Blob Storage and AWS S3 Multi-Cloud Storage Environments	130
--	-----

Yaser Mansouri, Adelaide University, Australia

Rajkumar Buyya, The University of Melbourne, Australia

Chapter 8

Intrusion Detection Systems for Internet of Things.....	148
---	-----

Gayathri K. S., Mar Baselios College of Engineering and Technology, India

Tony Thomas, Indian Institute of Information Technology and Management, Kerala, India

Chapter 9

Internal and External Threat Analysis of Anonymized Dataset	172
---	-----

Saurav Jindal, Punjab Engineering College, India

Poonam Saini, Punjab Engineering College, India

Chapter 10

A Comprehensive Survey on DDoS Attacks and Recent Defense Mechanisms	186
--	-----

Brij B. Gupta, National Institute of Technology, Kurukshetra, India

Amrita Dahiya, National Institute of Technology, Kurukshetra, India

Chivesh Upneja, National Institute of Technology, Kurukshetra, India

Aditi Garg, National Institute of Technology, Kurukshetra, India

Ruby Choudhary, National Institute of Technology, Kurukshetra, India

Chapter 11

A Legal Framework for Healthcare: Personal Data Protection for Health Law in Turkey	219
---	-----

Veli Durmuş, Marmara University, Turkey

Mert Uydaci, Marmara University, Turkey

Chapter 12

Auto Fill Security Solution Using Biometric Authentication for Fake Profile Detection in OSNs..... 237

Brij B. Gupta, National Institute of Technology, Kurukshetra, India

Somya Ranjan Sahoo, National Institute of Technology, Kurukshetra, India

Vaibhav Bhatia, National Institute of Technology, Kurukshetra, India

Adil Arafat, National Institute of Technology, Kurukshetra, India

Abhik Setia, National Institute of Technology, Kurukshetra, India

Chapter 13

An Attribute-Based Searchable Encryption Scheme for Non-Monotonic Access Structure 263

Mamta , National Institute of Technology, Kurukshetra, India

Brij B. Gupta, National Institute of Technology, Kurukshetra, India

Chapter 14

The State-of-the-Art Cryptography Techniques for Secure Data Transmission..... 284

Bhanu Chander, Pondicherry University, India

Chapter 15

Cloud Computing Security: Taxonomy of Issues, Challenges, Case Studies, and Solutions 306

Chhavi Chaturvedi, National Institute of Technology, Kurukshetra, India

Brij B. Gupta, National Institute of Technology, Kurukshetra, India

Chapter 16

Cybersecurity: An Emerging ICS Challenge 326

Selem Charfi, AUSY, France

Marko Mladenovic, UPHF LAMIH UMR 8201 CNRS, France

Chapter 17

Study of Smartcards Technology: Structure, Standards, Threats, Solutions, and Applications 341

Shaifali Narayan, National Institute of Technology, Kurukshetra, India

Brij B. Gupta, National Institute of Technology, Kurukshetra, India

Compilation of References 357

About the Contributors 399

Index 405

Detailed Table of Contents

Preface.....	xix
--------------	-----

Acknowledgment	xxiii
----------------------	-------

Chapter 1

Intelligent User Profiling Based on Sensors and Location Data to Detect Intrusions on Mobile Devices.....	1
---	---

Pedro Miguel Sánchez Sánchez, Universidad de Murcia, Spain

José María Jorquera Valero, Universidad de Murcia, Spain

Alberto Huertas Celdran, Waterford Institute of Technology, Ireland

Gregorio Martínez Pérez, Universidad de Murcia, Spain

Continuous authentication systems are considered as a promising solution to secure access to mobile devices. Their main benefit is the improvement of the users' experience when they use the services or applications of their mobile device. Specifically, continuous authentication avoids having to remember or possess any key to access an application or service that requires authentication. In this sense, having the user authenticated permanently increases the security of the device. It also allows the user interaction with applications to be much more fluid, simple, and satisfactory. This chapter proposes a new continuous authentication system for mobile devices. The system acquires data from the device sensors and the GPS location to create a dataset that represents the user's profile or normal behaviour. Then, the proposed system uses Machine Learning algorithms based on anomaly detection to perform user identification in real time. Several experiments have been carried out to demonstrate the performance and usefulness of the proposed solution.

Chapter 2

Improved Transmission of Data and Information in Intrusion Detection Environments Using the CBEDE Methodology.....	26
--	----

Reinaldo Padilha França, State University of Campinas (UNICAMP), Brazil

Yuzo Iano, State University of Campinas (UNICAMP), Brazil

Ana Carolina Borges Monteiro, State University of Campinas (UNICAMP), Brazil

Rangel Arthur, State University of Campinas (UNICAMP), Brazil

To anticipate threats, the Intrusion Detection System (IDS) enables the collection and use of information from various types of attacks to defend an entire network infrastructure. Therefore, this chapter develops a method of data transmission based on discrete event concepts, due to the fact that in this digitally globalized world, networks deal with a huge set of data all the time. Data refers to facts, events, actions,



PRINCIPAL

Alva's Institute of Engg. & Technology,
Majur. MOODBIDRI - 574 225, D.K.

activities, and transactions which have been and can be recorded, i.e., the raw material from which information is produced, nurturing the infrastructure and components that enable modern computing. This methodology was named CBEDE and experiments were matched in the MATLAB software, where the memory consumption was evaluated, presenting great potential to intermediate users and computer systems. Results showed better computational performance related to memory utilization related to the compression of the information, showing an improvement reaching up to 114.39%.

Chapter 3

Machine Learning Techniques for Intrusion Detection 47

Tameem Ahmad, Department of Computer Engineering, Z. H. College of Engineering and Technology, Aligarh Muslim University, Aligarh, India

Mohd Asad Anwar, Department of Computer Engineering, Z. H. College of Engineering and Technology, Aligarh Muslim University, Aligarh, India

Misbahul Haque, Department of Computer Engineering, Z. H. College of Engineering and Technology, Aligarh Muslim University, Aligarh, India

This chapter proposes a hybrid classifier technique for network Intrusion Detection System by implementing a method that combines Random Forest classification technique with K-Means and Gaussian Mixture clustering algorithms. Random-forest will build patterns of intrusion over a training data in misuse-detection, while anomaly-detection intrusions will be identified by the outlier-detection mechanism. The implementation and simulation of the proposed method for various metrics are carried out under varying threshold values. The effectiveness of the proposed method has been carried out for metrics such as precision, recall, accuracy rate, false alarm rate, and detection rate. The various existing algorithms are analyzed extensively. It is observed experimentally that the proposed method gives superior results compared to the existing simpler classifiers as well as existing hybrid classifier techniques. The proposed hybrid classifier technique outperforms other common existing classifiers with an accuracy of 99.84%, false alarm rate as 0.09% and the detection rate as 99.7%.


Chapter 4

Network Attack Detection With SNMP-MIB Using Deep Neural Network 66

Mouhammd Sharari Alkasassbeh, Computer Science Department, Princess Sumaya University for Technology, Jordan

Mohannad Zead Khairallah, Computer Science Department, Princess Sumaya University for Technology, Jordan

Over the past decades, the Internet and information technologies have elevated security issues due to the huge use of networks. Because of this advance information and communication and sharing information, the threats of cybersecurity have been increasing daily. Intrusion Detection System (IDS) is considered one of the most critical security components which detects network security breaches in organizations. However, a lot of challenges raise while implementing dynamics and effective NIDS for unknown and unpredictable attacks. Consider the machine learning approach to developing an effective and flexible IDS. A deep neural network model is proposed to increase the effectiveness of intrusions detection system. This chapter presents an efficient mechanism for network attacks detection and attack classification using the Management Information Base (MIB) variables with machine learning techniques. During the evaluation test, the proposed model seems highly effective with deep neural network implementation with a precision of 99.6% accuracy rate.


PRINCIPAL
Alva's Institute of Engg. & Technology,
Majar. MOOBBIDRI - 574 225, D.K

Chapter 5

A Survey on Detection and Analysis of Cyber Security Threats Through Monitoring Tools..... 77

Manjunath Kotari, Alva's Institute of Engineering and Technology, Moodbidri, India

Niranjana N. Chiplunkar, NMAM Institute of Technology, Nitte, India

Cyber crime is a serious threat for day-to-day transactions of the digital life. Overexposure of the personal details in social networks will lead to the cyber crime case. Therefore, detection and monitoring of cyber crime are challenging tasks. The cyber criminals are continually flooding the various intrusions all over the network. The cyber safety team should have a noteworthy challenge of filtering various such information. Continuous nonstop cyberattacks or intrusion examinations by security tools will significantly improve the threat alerts. However, cyber security becomes more expensive in the case of the above methods. The chapter provides systematic survey of various cyber security threats, evolution of intrusion detection systems, various monitoring mechanisms, open source cyber security monitoring tools, and various assessment techniques. The chapter also proposes a model of Cyber security detection and monitoring system and its challenges.

Chapter 6

Identification and Classification of Cyber Threats Through SSH Honeypot Systems..... 105

*José María Jorquera Valero, Department of Information and Communications Engineering,
University of Murcia, Spain*

*Manuel Gil Pérez, Department of Information and Communications Engineering, University
of Murcia, Spain*

*Alberto Huertas Celdrán, Telecommunications Software and Systems Group, Waterford
Institute of Technology, Ireland*

*Gregorio Martínez Pérez, Department of Information and Communications Engineering,
University of Murcia, Spain*

As the number and sophistication of cyber threats increases year after year, security systems such as antivirus, firewalls, or Intrusion Detection Systems based on misuse detection techniques are improved in detection capabilities. However, these traditional systems are usually limited to detect potential threats, since they are inadequate to spot zero-day attacks or mutations in behaviour. Authors propose using honeypot systems as a further security layer able to provide an intelligence holistic level in detecting unknown threats, or well-known attacks with new behaviour patterns. Since brute-force attacks are increasing in recent years, authors opted for an SSH medium-interaction honeypot to acquire a log set from attacker's interactions. The proposed system is able to acquire behaviour patterns of each attacker and link them with future sessions for early detection. Authors also generate a feature set to feed Machine Learning algorithms with the main goal of identifying and classifying attacker's sessions, and thus be able to learn malicious intentions in executing cyber threats.

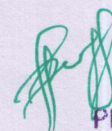
Chapter 7

Data Access Management System in Azure Blob Storage and AWS S3 Multi-Cloud Storage Environments 130

Yaser Mansouri, Adelaide University, Australia

Rajkumar Buyya, The University of Melbourne, Australia

Multi-cloud storage offers better Quality of Service (QoS) such as availability, durability, and users' perceived latency. The exploitation of price differences across cloud-based storage services is a motivate



PRINCIPAL

Alva's Institute of Engg. & Technology,
Moodbidri - 574 225, D.K.

example of storing data in different Geo-graphically data stores, where data migration is also a choice to achieve more cost optimization. However, this requires migrating data in tolerable time from the perspective of users. This chapter first proposes a comprehensive review on different classes of data stores inspiring data migration within and across data stores. Then, it presents the design of a system prototype spanned across storage services of Amazon Web Services (AWS) and Microsoft Azure employing their RESTful APIs to store, retrieve, delete, and migrate data. Finally, the experimental results show that the data migration can be conducted in a few seconds for data with a magnitude of Megabytes.

Chapter 8

Intrusion Detection Systems for Internet of Things 148

Gayathri K. S., Mar Baselios College of Engineering and Technology, India

Tony Thomas, Indian Institute of Information Technology and Management, Kerala, India

Internet of things (IoT) is revolutionizing this world with its evolving applications in various aspects of life such as sensing, healthcare, remote monitoring, and so on. These systems improve the comfort and efficiency of human life, but the inherent vulnerabilities in these IoT devices create a backdoor for intruders to enter and attack the entire system. Hence, there is a need for intrusion detection systems (IDSs) designed for IoT environments to mitigate IoT-related security attacks that exploit some of these security vulnerabilities. Due to the limited computing and storage capabilities of IoT devices and the specific protocols used, conventional IDSs may not be an option for IoT environments. Since the security of IoT systems is critical, this chapter presents recent research in intrusion detection systems in IoT systems.

Chapter 9

Internal and External Threat Analysis of Anonymized Dataset 172

Saurav Jindal, Punjab Engineering College, India

Poonam Saini, Punjab Engineering College, India

In recent years, data collection and data mining have emerged as fast-paced computational processes as the amount of data from different sources has increased manifold. With the advent of such technologies, major concern is exposure of an individual's self-contained information. To confront the unusual situation, anonymization of dataset is performed before being released into public for further usage. The chapter discusses various existing techniques of anonymization. Thereafter, a novel redaction technique is proposed for generalization to minimize the overall cost (penalty) of the process being inversely proportional to utility of generated dataset. To validate the proposed work, authors assume a pre-processed dataset and further compare our algorithm with existing techniques. Lastly, the proposed technique is made scalable thus ensuring further minimization of generalization cost and improving overall utility of information gain.

Chapter 10

A Comprehensive Survey on DDoS Attacks and Recent Defense Mechanisms 186

Brij B. Gupta, National Institute of Technology, Kurukshetra, India

Amrita Dahiya, National Institute of Technology, Kurukshetra, India

Chivesh Upneja, National Institute of Technology, Kurukshetra, India

Aditi Garg, National Institute of Technology, Kurukshetra, India

Ruby Choudhary, National Institute of Technology, Kurukshetra, India

DDoS attack always takes advantage of structure of Internet and imbalance of resources between defender and attacker. DDoS attacks are driven by factors like interdependency of Internet's security, limited

resources, fewer incentives for home users and local ISPs, flexibility of handlers to control multiple compromised systems at the same time, untraceable nature of malicious packets and unfair distribution of resources all over the Internet. This survey chapter gives a comprehensive view on DDoS attacks and its defense mechanisms. Defense mechanisms are categorized according to the deployment position and nature of defense. Comprehensive study of DDoS attacks will definitely help researchers to understand the important issues related to cyber security.

Chapter 11

A Legal Framework for Healthcare: Personal Data Protection for Health Law in Turkey 219

Veli Durmuş, Marmara University, Turkey

Mert Uydaci, Marmara University, Turkey

This chapter provides a holistic general overview of the data protection regime in Turkey. Authors present the principal rights of data protection and transmission in health law and latent ethical concerns by specifying decisions of the Supreme Court in Turkey and the European Court of Human Rights on using personal data. The research describes data protection law for health care setting in Turkey. Primary and secondary data have been used for the study. The primary data includes the information collected with current national and international regulations or law. Secondary data include publications, books, journals, and empirical legal studies. Privacy and data protection regimes in health law show there are some obligations, principles, and procedures which shall be binding upon natural or legal persons who process health-related personal data.

Chapter 12

Auto Fill Security Solution Using Biometric Authentication for Fake Profile Detection in OSNs..... 237

Brij B. Gupta, National Institute of Technology, Kurukshetra, India

Somya Ranjan Sahoo, National Institute of Technology, Kurukshetra, India

Vaibhav Bhatia, National Institute of Technology, Kurukshetra, India

Adil Arafat, National Institute of Technology, Kurukshetra, India

Abhik Setia, National Institute of Technology, Kurukshetra, India

This chapter discusses a model that allows the user to access social networking sites through login using smart phone-based biometric authentication. Currently, social networking websites permit the user to access their page through login and some sites provide auto fill system to login into users account through browser by permit. The browser saves the password in password protected space and automatically auto fills the password to access the account by user. This facility is not highly reliable due to the auto fill system for laptop users. When someone uses the laptop of others and visits any website, the auto fill system opens the content with saved password. Secondly, elderly people have problems logging into today's websites. To remember the password for every account is very difficult for elderly people. This chapter describes a model for security and authenticity. Authors used a hybrid model with android as the application with fingerprint authentication and chrome extension as the auto fill process for user access.

Chapter 13

An Attribute-Based Searchable Encryption Scheme for Non-Monotonic Access Structure 263

Mamta , National Institute of Technology, Kurukshetra, India

Brij B. Gupta, National Institute of Technology, Kurukshetra, India

Attribute based encryption (ABE) is a widely used technique with tremendous application in cloud computing because it provides fine-grained access control capability. Owing to this property, it is emerging as a popular technique in the area of searchable encryption where the fine-grained access control is used to determine the search capabilities of a user. But, in the searchable encryption schemes developed using ABE it is assumed that the access structure is monotonic which contains AND, OR and threshold gates. Many ABE schemes have been developed for non-monotonic access structure which supports NOT gate, but this is the first attempt to develop a searchable encryption scheme for the same. The proposed scheme results in fast search and generates secret key and search token of constant size and also the ciphertext components are quite fewer than the number of attributes involved. The proposed scheme is proven secure against chosen keyword attack (CKA) in selective security model under Decisional Bilinear Diffie-Hellman (DBDH) assumption.

Chapter 14

The State-of-the-Art Cryptography Techniques for Secure Data Transmission 284

Bhanu Chander, Pondicherry University, India

Cryptography is a progression where message correspondences are intelligently sent from one abuser to an additional abuser which endows with frequent defense services like privacy, data truthfulness, or verification to the wireless transportation structure. An encryption method keeps exceptional crucial contribution to communication safety measures. Here we mentioned characteristics of various Symmetric and Asymmetric encryption techniques along with inclusion of optimization techniques in cryptography for decrease computation difficulty. Moreover, advanced encryption techniques such as Zero-knowledge, Multi-party, Homomorphism encryptions, and Cognitive cryptography, Blockchain with their associated protocols are described. The present day's extensive research practices on quantum computer machines explain mathematical tribulations which are complicated or stubborn for classical computers. Quantum cryptography, challenges, Goal of Quantum resistant cryptography with associated literature work is described.

Chapter 15

Cloud Computing Security: Taxonomy of Issues, Challenges, Case Studies, and Solutions 306

Chhavi Chaturvedi, National Institute of Technology, Kurukshetra, India

Brij B. Gupta, National Institute of Technology, Kurukshetra, India

The applications and software using cloud computing as a base have significantly increased, and cloud computing is nowadays developed as a scalable and cost-effective technique. It facilitates many features in the computing environment like resource pooling, multi-tenancy, virtualization, etc. The cloud environment has led to the proliferation of various attacks that affect the security of applications and software developed by using cloud services and also cloud user's data. Data security is the main concern in cloud computing because it is stored in data centers provided by service providers. The chapter presents the background history of cloud computing and different challenges faced by the cloud environment, especially in terms of providing security for customer data stored in data centers. Authors also discuss the case studies on Microsoft Azure (i.e. a cloud platform) and Aneka (i.e. a cloud development and management platform).

Chapter 16

Cybersecurity: An Emerging ICS Challenge.....	326
---	-----

Selem Charfi, AUSY, France

Marko Mladenovic, UPHF LAMIH UMR 8201 CNRS, France

Cybersecurity is generally considered as an information security topic, often associated with personal data and information databases: collecting, exposing, corrupting, or deleting these data. However, it is a more global problem, and related to broader aspects, such as controlling cyber-systems. In ICS, the topic of cybersecurity is considered at the operational and responsible level as a secondary threat, and much more as an IT problem. This premise has proven to lead to substantial losses. For example, dangerous aspects in some installation can stress the cybersecurity in ICS, for instance, plants dealing with hazardous materials, as the attackers can take over control of the production lines. This chapter encapsulates points in common on the topic of cybersecurity in IT and ICS. IT has already devoted significant resources into cyber-threats. ICS has yet to do so. To do so, authors review a number of papers dealing with the same topic.

Chapter 17

Study of Smartcards Technology: Structure, Standards, Threats, Solutions, and Applications	341
--	-----

Shaifali Narayan, National Institute of Technology, Kurukshetra, India

Brij B. Gupta, National Institute of Technology, Kurukshetra, India

Smart cards have gained popularity in many domains by providing different facilities in every domain. Such cards are beneficial for storing credentials and access information. The cards are easy to carry and provides easy and fast computations. The cards have certain limitations due to the possible attacks on them. This chapter gives an overview of the smartcards including its history, physical design, life cycle. It also provides an overview of the possible threats on smartcards and its application area.

Compilation of References	357
---------------------------------	-----

About the Contributors	399
------------------------------	-----

Index.....	405
------------	-----

Chapter 5

A Survey on Detection and Analysis of Cyber Security Threats Through Monitoring Tools

Manjunath Kotari

Alva's Institute of Engineering and Technology, Moodbidri, India

Niranjana N. Chiplunkar

NMAM Institute of Technology, Nitte, India

ABSTRACT

Cyber crime is a serious threat for day-to-day transactions of the digital life. Overexposure of the personal details in social networks will lead to the cyber crime case. Therefore, detection and monitoring of cyber crime are challenging tasks. The cyber criminals are continually flooding the various intrusions all over the network. The cyber safety team should have a noteworthy challenge of filtering various such information. Continuous nonstop cyberattacks or intrusion examinations by security tools will significantly improve the threat alerts. However, cyber security becomes more expensive in the case of the above methods. The chapter provides systematic survey of various cyber security threats, evolution of intrusion detection systems, various monitoring mechanisms, open source cyber security monitoring tools, and various assessment techniques. The chapter also proposes a model of Cyber security detection and monitoring system and its challenges.

1. INTRODUCTION

Cyber security threats are major hurdle for the development activities of the Information Technology (IT) industry. The IT industry is facing severe crisis of cyber-crime activities in their business. A large set of data and assets of organizations are placed in cloud-based platform. The virtual cloud computing is facing various threats which include, Intrusions, Malwares, and Mining of Crypto currency. The

DOI: 10.4018/978-1-7998-2242-4.ch005


PRINCIPAL

Alva's Institute of Engg. & Technology,
Moodbidri - 574 225, D.K

Virtual Machines faces intrusions and impersonations in the cloud environments. The bitcoin attracts more severe cyber crimes. This can be illustrated in cloud computing by layer wise cyber attacks. Cyber Security (Gupta, Agrawal, & Wang, 2019) is becoming a very important concern for the functioning of web applications. The rising cost of cyber security damages reflects a failure of the security field to offer a solution that is both simple enough to warrant adoption by industry and government and secure enough to protect our valuable assets and data. Most of the organizations are facing shortage of cyber security professionals to monitor the user activities in day to day life. However, IT organizations may use various tools and technologies to maintain privacy of user data. Most of the corporate information security (Quhtani, 2017) is analyzed by data mining applications. In the corporate world, marketing campaign surveys are analyzed according to data mining applications. The objective of this chapter is to provide the comprehensive survey on detection and analysis of various cyber security threats exists in the web applications and network. The chapter also reviews the various open source security monitoring tools with classifications. The challenges faced by cyber-security tools have been included for the purpose of providing future solutions. The architecture of cyber-security threat detection and monitoring system to analyze the working of cyber-security tools has been proposed in this chapter.

1.1 Cyber Security Monitoring

Security monitoring is the collection of data from a range of security systems and the correlation and analysis of this information with threat intelligence to identify signs of compromise. Cyber-Security monitoring is an essential part of cyber risk management systems, which enables the company networks to detect cyber hackers in their early life, and quickly shoot up threats for healing before they cause harm and interference. Baselineing is the process of establishing an agreed level of typical network performance. It plays an important role in cyber security monitoring. Any network behavior that falls outside what is considered regular behavior should be analyzed to identify whether or not it could be malicious.

1.2 How Does Cyber Security Monitoring Work?

Cyber security analysts will utilise a range of technologies to achieve visibility of threats. There are two types of monitoring, viz., network security monitoring and endpoint security monitoring. Network security monitoring tools comprise Security Information and Event Management (SIEM) and Intrusion Detection Systems (IDS). SIEM systems collect, manage and correlate log information from a range of sources to provide a holistic view of security posture, and generate alerts for investigation by cyber security analysts. IDS combines network (NIDS) and host (HIDS) based methods to analyse network traffic and identify anomalous behaviour. Endpoint security monitoring technologies provide visibility of activity such as file read, write, executions and registry changes across desktops, laptops, and servers.

1.3 Challenges of In-House Security Monitoring

Basically all the security monitoring tools generates enormous number of alert messages. Filtering of alert messages to identify true threats from false positives is hassle task. In that case, essential alerts may be ignored during the monitoring process. Hence, setting up of new Cyber Security Operations Centre (CSOC) is essential. However, CSOC is more expensive. Instead of recruiting, training and managing

26 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the product's webpage:

www.igi-global.com/chapter/a-survey-on-detection-and-analysis-of-cyber-security-threats-through-monitoring-tools/251798?camid=4v1

This title is available in Advances in Information Security, Privacy, and Ethics, InfoSci-Books, InfoSci-Computer Science and Information Technology, Science, Engineering, and Information Technology, InfoSci-Security and Forensics, InfoSci-Select, InfoSci-Computer Science and IT Knowledge Solutions – Books. Recommend this product to your librarian:

www.igi-global.com/e-resources/library-recommendation/?id=96

Related Content

Emerging Information Technology Issues in Higher Education

Sarah Axtell and Tutaleni I. Asino (2020). *IT Issues in Higher Education: Emerging Research and Opportunities* (pp. 1-16).

www.igi-global.com/chapter/emerging-information-technology-issues-in-higher-education/237662?camid=4v1a

Without Permission: Privacy on the Line

Joanne H. Pratt and Sue Conger (2009). *International Journal of Information Security and Privacy* (pp. 30-44).

www.igi-global.com/article/without-permission-privacy-line/4000?camid=4v1a

Smartphone Confrontational Applications and Security Issues

Abhishek Kumar, Jyotir Moy Chatterjee and Pramod Singh Rathore (2020). *International Journal of Risk and Contingency Management* (pp. 1-18).

www.igi-global.com/article/smartphone-confrontational-applications-and-security-issues/246844?camid=4v1a

Factors Influencing College Students' Use of Computer Security

Norman Pendegraft, Mark Rounds and Robert W. Stone (2012). *Optimizing Information Security and Advancing Privacy Assurance: New Technologies* (pp. 225-234).

www.igi-global.com/chapter/factors-influencing-college-students-use/62725?camid=4v1a


PRINCIPAL
Jyoti's Institute of Engg. & Technology,
Majur, MOOUBIDRI - 574 225, D.K