

About the Book

Foundation of Computer Security: Cryptography, Attacks, and Emerging Technologies" is a comprehensive guide to cybersecurity in the digital age. Covering topics from cryptography to emerging technologies like IoT and blockchain, this book offers insights and practical advice for professionals, researchers, and students. It explores secure communication, network security, AI in cybersecurity, healthcare security, cloud security, and the potential of emerging technologies to enhance security measures. With a focus on theoretical understanding and practical applications, it's an essential resource for navigating the ever-evolving landscape of computer security.

About the Editors:

Dr. Manish Tiwari is serving as Associate Professor and Head, Department of Computer Science and Engineering, Career Point University, Kota, Rajasthan, India. His research interests include Artificial Intelligence, Data Mining. He has 1 books, 25 publications National, International and Conferences, 12 filed Indian patents in his credit. Till date 6 students are doing PhD work under his guidance, 12 students have successfully obtained their M.Tech degree under his sole supervision as Supervisor.

Mr. Rohit Maheshwari an esteemed academician, possesses an extensive 18 years of experience in the education sector. Currently engaged in the pursuit of a PhD in computer science, his academic interests encompass Network Security, Artificial Intelligence, and Machine Learning. Mr. Maheshwari holds the position of Assistant Professor at Career Point University in Kota, Rajasthan.

Deepak Mahawar has dedicated over 19 years to academia, showcasing versatility and a pursuit of excellence. He holds a Bachelor's in Computer Science & Engineering, a Master's in Technology, and is pursuing a Ph.D. in Computer Science and Artificial Intelligence. His career includes research roles at Indian Institute of Technology, Kanpur, with publications and presentations in international forums. As an educator, he has contributed to institutions like Poornima University, Suresh Gyan Vihar University, and Career Point University, focusing on curriculum development and student mentorship.

Ms. Preeti Gupta an esteemed academician, possesses an extensive 17 years of experience in the education sector. She has accomplished her master of technology in Computer Science. Her academic interests encompass Information Security and Artificial Intelligence. Ms. Gupta holds the position of Assistant Professor at Career Point University Kota, Rajasthan.

As an educator, she has contributed to institutions like Modi Institute of Technology Kota, Jodhpur Institute of Engineering and Technology Jodhpur and Career Point University, focusing on curriculum development and student mentorship.



FOUNDATION OF COMPUTER SECURITY

cryptology, Attacks and Emerging Technologies



Editor:
Manish Tiwari
Rohit Maheshwari
Deepak Mahawar
Preeti Gupta

FOUNDATION OF COMPUTER SECURITY

CRYPTOGRAPHY, ATTACKS AND EMERGING TECHNOLOGIES

Information contained in this work has been obtained by Career Point from sources believed to be reliable. However, neither Career Point nor its authors guarantee the accuracy or completeness of any information published herein, and neither Career Point nor its authors shall be responsible for any errors, omissions, or damages arising out of use of this information. This work is published with the understanding that Career Point and its authors are supplying information but are not attempting to render any professional services. If such services are required, the assistance of an appropriate professional should be sought.

CAREER POINT

CP Tower, Road No.-1, IPIA, Kota (Raj.)

Email : publication@cpil.in

No part of this publication may be reproduced or distributed in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise or stored in a database or retrieval system without the prior written permission of the Publishers. The program listings (if any) may be entered, stored and executed in a computer system, but they may not be reproduced for publication.

This edition can be exported from India only by the publisher.

Published by Career Point Ltd.
CP Tower, Road No.-1, IPIA, Kota (Raj.)
Email : publication@cpil.in

Book No. : CPP-706

Preface

In today's digital age, computer security is of utmost importance as technology pervades every aspect of our lives. This book offers a comprehensive exploration of computer security, covering topics from cryptography to emerging technologies like IoT, AI, cloud computing, and blockchain.

Beginning with cryptography, we delve into the fundamentals of secure communication, exploring classical encryption methods and modern cryptographic algorithms. We then move on to network security, discussing advancements and strategies to safeguard interconnected systems against cyber threats.

The section on IoT security addresses the unique challenges posed by the interconnectedness of devices, offering strategies for securing IoT ecosystems. AI's role in cybersecurity is examined, highlighting how machine learning can automate threat detection and response effectively.

A focus on healthcare security introduces a technique using AI for secure image watermarking to protect sensitive medical data. Cloud security best practices are outlined, covering encryption, access control, and threat detection in cloud environments.

Emerging technologies like quantum computing and blockchain are explored for their potential to enhance cloud security. Finally, we discuss blockchain's applications beyond cryptocurrency, offering transparency, immutability, and security in various industries.

This book is tailored for cybersecurity professionals, researchers, and students, providing theoretical insights and practical guidance to navigate the evolving landscape of cyberspace effectively.



Book Description

"Foundation of Computer Security: Cryptography, Attacks, and Emerging Technologies" is a comprehensive guide to cybersecurity in the digital age. Covering topics from cryptography to emerging technologies like IoT and blockchain, this book offers insights and practical advice for professionals, researchers, and students. It explores secure communication, network security, AI in cybersecurity, healthcare security, cloud security, and the potential of emerging technologies to enhance security measures. With a focus on theoretical understanding and practical applications, it's an essential resource for navigating the ever-evolving landscape of computer security.

Table of Contents

CHAPTERS TITLES	Page No.
Chapter 1. Computer Security Mr. Deepak Mahawar Abstract: This chapter provides a comprehensive overview of computer security, covering its necessity, approaches, principles, and common types of attacks. It emphasizes the critical importance of safeguarding digital information in today's interconnected world, detailing preventive, detective, corrective, and proactive security measures. Fundamental principles such as confidentiality, integrity, and availability guide the design of secure systems. The chapter explores various types of attacks, including malware, phishing, and denial-of-service, along with preventive measures such as antivirus software and email filtering. Additionally, specific threats like sniffing and spoofing, phishing, pharming, and DNS spoofing are discussed, accompanied by corresponding countermeasures to mitigate their risks.	1-8
Chapter 2. Cryptography: Concepts and Techniques Mr. Deepak Mahawar Abstract: The chapter on "Cryptography: Concepts and Techniques" provides a foundational overview of cryptographic principles, historical developments, and practical applications. It covers topics such as symmetric and asymmetric encryption, hash functions, cryptographic protocols, and various types of ciphers including substitution, transposition, and polyalphabetic ciphers. Through concise explanations and examples, the chapter offers readers a comprehensive understanding of cryptography's importance in ensuring data security and privacy.	9-16
Chapter 3. Cryptography and Secure Communication: A Comprehensive Overview Mr. Deepak Mahawar Abstract: The chapter "Cryptography and Secure Communication: A Comprehensive Overview" delves into the vital role of cryptographic techniques and secure communication protocols in today's interconnected digital landscape. It covers topics such as symmetric and asymmetric key cryptography, block and stream ciphers, digital signatures, message digests, internet security protocols, and email security. Through real-world examples and emerging trends, readers gain insights into navigating complexities to uphold security standards in the digital age.	17-26
Chapter 4. Advancements in Network Security: A Comprehensive Overview Dr. Manish Tiwari, Siddharth Kumar Abstract: Network security represents a highly specialized domain encompassing regulations and protocols aimed at thwarting and overseeing unauthorized entry, alteration, obstruction or misuse of a computer network and its accessible resources. Additionally, it ensures the availability of these resources through meticulous procedures. A multitude of security apparatus is under development and implementation to counter cyber threats and forestall inadvertent data breaches. Despite these collective endeavours, the era colloquially known as the 'golden age' of cybercrime endures, with organizations worldwide grappling with persistent data breaches and security assaults. In the face of this ongoing challenge, it is imperative to examine the nature of contemporary	27-36

CHAPTERS TITLES	Page No.
<p>threats and formulate effective strategies for mitigation. This paper aims to deliver an updated perspective on network security for both organizations and researchers in the field. Furthermore, it endeavours to offer recommendations to address the current landscape of security threats, providing insights into the types of challenges faced today and proposing measures for effective response and prevention.</p>	
<p>Chapter 5. Emerging Trends and Technologies: Internet of Things (IoT) Security Mr. Deepak Mahawar Abstract: The chapter on "Emerging Trends and Technologies: Internet of Things (IoT) Security" delves into the critical aspects of securing connected devices and networks in the era of IoT proliferation. It begins by contextualizing the evolving cybersecurity landscape, emphasizing the significance of addressing new challenges posed by emerging technologies like IoT. Subsequently, it explores the multifaceted dimensions of IoT security, highlighting the transformative potential of IoT while underscoring the pressing need to mitigate associated risks. By dissecting the components, evolution, and applications of IoT ecosystems, the chapter elucidates the intricate interplay between technological innovation, market dynamics, and security imperatives.</p>	<p>37-43</p>
<p>Chapter 6. Security Automation with AI Dr. Manish Tiwari, Keshav Sharma Abstract: By providing a dynamic and proactive defense against ever-evolving threats, the integration of Artificial Intelligence (AI) into security automation is fundamentally changing the cybersecurity landscape. This investigation explores the core ideas, advantages, factors, and potential directions of this collaboration. AI strengthens security postures and speeds up response times with its abilities in behavioral analysis, enhanced threat detection, and predictive analytics. Despite the significant advantages, there are still obstacles to overcome, including balancing issues between humans and machines, ongoing monitoring, and ethical issues. Future predictions include hyper-automation, autonomous operations, and explainable AI, which will usher in a robust period where human expertise and intelligent automation work together to protect digital ecosystems. This trip highlights how important it is for businesses to include AI into their cybersecurity plans, paving the way for improved resilience and flexibility in</p>	<p>44-48</p>
<p>Chapter 7. A Secure Image Watermarking Technique for Healthcare Using Artificial Intelligence Ms.Preeti Gupta Abstract : Watermarking using AI involves embedding digital watermarks into multimedia content, such as images, videos, or audio, to protect intellectual property, indicate ownership, or track the source of the content. AI-based watermarking -techniques often leverage advanced algorithms to ensure robustness, imperceptibility, and resistance against removal or tampering. The proposed technique leverages advanced watermarking algorithms to embed imperceptible and robust watermarks directly into medical images, ensuring the integrity and authenticity of the visual data. The primary objectives of this technique include protecting patient confidentiality, preventing unauthorized tampering, and facilitating the traceability of medical images” throughout their lifecycle.</p>	<p>49-55</p>

CHAPTERS TITLES	Page No.
<p>Chapter 8. Security Best Practices for Cloud Infrastructure</p> <p>Dr. Manish Tiwari, Tripti Verma</p> <p>Abstract : Cloud computing has become an indispensable element of modern IT infrastructure, offering scalability, flexibility, and cost-effectiveness. However, the dynamic nature of cloud environments and the proliferation of cyber threats present significant security challenges. This abstract examines the key issues in cloud security and proposes strategies to fortify cloud infrastructures.</p> <p>One of the foremost challenges in cloud security is data protection. With sensitive information stored in remote servers, ensuring confidentiality, integrity, and availability is paramount. Encryption, robust access controls, and regular data audits are essential measures to safeguard against unauthorized access and data breaches.</p> <p>The shared responsibility model complicates security efforts, requiring collaboration between cloud providers and customers. While providers manage the underlying infrastructure, customers are responsible for securing their data and applications. Establishing clear roles and responsibilities, implementing comprehensive security policies, and conducting regular security assessments are vital for maintaining a secure environment.</p>	<p>56-62</p>
<p>Chapter 9. Ensuring the Security with Emerging Technologies and Trends in Cloud</p> <p>Dr. Manish Tiwari</p> <p>Abstract: Recent scenarios the cloud is going to take an important part of every industry and the person. Cloud is going to reduce the infrastructure cost to set up any IT infrastructure. Nowadays many companies provide the cloud infrastructure for providing the services to different industries at different cost such as Amazon serves as AWS cloud, Microsoft provides the cloud services as AZURE, Google cloud etc. As the demand of the cloud is increasing and many industries are preferring cloud to store their data and different level services to the customer as the security risk (authentication, Repudiation, data breach etc.) also is going to be increased. This chapter is going to denote the type of problem that occurs.</p>	<p>63-68</p>
<p>Chapter 10. Blockchain Beyond Bitcoin: Exploring Recent Technological Advancements and Industry Adoption</p> <p>Mr. Rohit Maheshwari, Mahak Kaur Chhabra</p> <p>Abstract:The paper provides a concise overview of blockchain technology, covering its principles, evolution, recent advancements, industry applications, challenges, and transformative potential. It highlights key topics such as decentralization, Bitcoin's role, recent technological developments, industry-specific applications, and challenges like scalability and energy consumption. Ultimately, it emphasizes blockchain's promise in reshaping digital ecosystems for enhanced security, efficiency, and inclusivity.</p>	<p>69-76</p>

Editors

Dr. Manish Tiwari

Associate Professor & HOD

Department of Computer Science and Engineering, Career Point University, Kota

Mr. Rohit Maheshwari

Assistant Professor,

Computer Science and Engineering, Career Point University, Kota

Mr. Deepak Mahawar

Assistant Professor

Department of Computer Science and Engineering, Career Point University, Kota

Ms. Preeti Gupta

Assistant Professor,

Computer Science and Engineering, Career Point University, Kota

About the Editors:

Dr. Manish Tiwari, is serving as Associate Professor and Head, Department of Computer Science and Engineering, Career Point University, Kota, Rajasthan, India. His research interests include Artificial Intelligence, Data Mining. He has 1 books, 25 publications National, International and Conferences, 12 filed Indian patents in his credit. Till date 6 students are doing PhD work under his guidance, 12 students have successfully obtained their M.Tech degree under his sole supervision as Supervisor.

Mr. Rohit Maheshwari, an esteemed academician, possesses an extensive 18 years of experience in the education sector. Currently engaged in the pursuit of a PhD in computer science, his academic interests encompass Network Security, Artificial Intelligence, and Machine Learning. Mr. Maheshwari holds the position of Assistant Professor at Career Point University Kota, Rajasthan.

Deepak Mahawar has dedicated over 19 years to academia, showcasing versatility and a pursuit of excellence. He holds a Bachelor's in Computer Science & Engineering, a Master's in Technology, and is pursuing a Ph.D. in Computer Science and Artificial Intelligence. His career includes research roles at Indian Institute of Technology, Kanpur, with publications and presentations in international forums.

As an educator, he has contributed to institutions like Poornima University, Suresh Gyan Vihar University, and Career Point University, focusing on curriculum development and student mentorship. Deepak has enhanced his skills in areas like entrepreneurship and mobile computing and has actively participated in organizational activities.

Ms. Preeti Gupta, an esteemed academician, possesses an extensive 17 years of experience in the education sector. She has accomplished her master of technology in Computer Science. Her academic interests encompass Information Security and Artificial Intelligence. Ms. Gupta holds the position of Assistant Professor at Career Point University Kota, Rajasthan.

As an educator, she has contributed to institutions like Modi Institute of Technology Kota, Jodhpur Institute of Engineering and Technology Jodhpur and Career Point University, focusing on curriculum development and student mentorship.

Advancements in Network Security A Comprehensive Overview

Dr. Manish Tiwari, Siddharth Kumar

ABSTRACT

Network security represents a highly specialized domain encompassing regulations and protocols aimed at thwarting and overseeing unauthorized entry, alteration, obstruction or misuse of a computer network and its accessible resources. Additionally, it ensures the availability of these resources through meticulous procedures. A multitude of security apparatus is under development and implementation to counter cyber threats and forestall inadvertent data breaches. Despite these collective endeavours, the era colloquially known as the 'golden age' of cybercrime endures, with organizations worldwide grappling with persistent data breaches and security assaults.

In the face of this ongoing challenge, it is imperative to examine the nature of contemporary threats and formulate effective strategies for mitigation. This paper aims to deliver an updated perspective on network security for both organizations and researchers in the field. Furthermore, it endeavours to offer recommendations to address the current landscape of security threats, providing insights into the types of challenges faced today and proposing measures for effective response and prevention.

Content-

1. Introduction
2. Security threats
3. Descriptions of various threats of their motivations are given as follows
4. Instances of insider attacks also occurred
5. Social Networking and Other Vulnerabilities
6. User-Involved Attacks
7. Emerging Patterns in Cybersecurity
8. Cyber activism
9. Compromised Information Integrity
10. Conclusion

1. Introduction:

In the contemporary era, the Internet has witnessed a significant amount of growth in terms of usage and resources, becoming an indispensable tool for major commercial organizations, educational institutions, governments, and individuals. The exchange of information, collaboration, and the dissemination of knowledge have become reliant on the Internet across various sectors. Commercial organizations use it for communication with partners and clients, educational institutes

share study materials, governments provide information to citizens, and individuals utilize it for accessing information, online shopping, and communication through emails and social networking.

The Internet serves as a crucial platform for running services and storing sensitive information for organizations and individuals alike. However, the increasing dependence on the Internet also brings about challenges, particularly in terms of security. Configuration errors and vulnerabilities in widely-used software create opportunities for malicious users to launch cyber-attacks, aiming to disrupt services and compromise the integrity of sensitive information. These deliberate exploits involve the use of malicious code to alter computer systems, networks, and enterprises, leading to destructive consequences that can jeopardize information security.

One significant concern is the existence of zero-day vulnerabilities, associated with newly published programs or web services, which can be particularly harmful as they remain unknown until patched. Exploitation of such vulnerabilities provides attackers with more opportunities to compromise systems. For instance, attacks on major tech companies like Microsoft, Facebook, and Twitter, Apple have exploited vulnerabilities in Java. Outdated software versions, misconfigurations in network elements, and server vulnerabilities further contribute to the risk landscape, allowing for unauthorized access, data theft, and modification of websites.

To mitigate these risks, network security devices are equipped with various security functions, including firewalls, intrusion prevention systems/intrusion detection systems (IPS/IDS), data loss prevention (DLP), and content security filtering functions like anti-spam, antivirus, or URL filtering. Despite these measures, achieving 100% security is acknowledged as an unattainable goal, given the dynamic nature of cyber threats. The evolving landscape, marked by trends like cloud computing, user mobility, and Bring Your Own Device (BYOD), adds complexity to security challenges, expanding the attack surface and diminishing the effectiveness of traditional defenses.

The paper underlines the persistent nature of the new war involving advanced threat and attack as sensitive information continues to grow across data centres, servers, PCs, and mobile phones. It emphasizes the challenges posed by rapidly changing attack trends, the inadequacy of conventional techniques, and the need for effective security policies. The analysis of latest network security events and prominent attacks worldwide is followed by recommendations on protecting against such assaults. The paper concludes by asserting that only through the integration of security-intelligence and user training can organizations effectively defend against evolving cyber threats.

2. Security threats:

The increasing dependence of organizations and individuals on the Internet is accompanied by a growing risk of cyber threats. Popular software often contains vulnerabilities and configuration errors that are technically challenging and economically costly to address. Intruders exploit these weaknesses and easy internet access to launch attacks, including Denial of Service (DoS) and Information attacks. The annual revelation of over 5000 new hacking methods in 2012 alone underscores the magnitude of the problem. Figure 2 illustrates that widely used products, such as those from Oracle, Apple, and Microsoft, were highly susceptible to cyber-attacks in 2012. Research from Check Point Software Technologies indicates that a significant portion of organizational hosts did not use the latest software versions or Microsoft Windows Service Packs, exposing them to security risks. Addressing these vulnerabilities is crucial to enhancing cybersecurity.

Panda Labs' 2012 annual report highlights a continuous increase in the circulation of Trojans over the preceding years. In 2012, Trojans accounted for 76.57% of all malware, marking a significant rise from 56% in 2010 and 73.31% in 2011. This dominance is attributed to cyber-criminals infecting more computers with Trojans, facilitated by the use of exploit kits like black hole that exploit system vulnerabilities automatically. The availability of free, user-friendly attack tools on the Internet, such as Stacheldraht and Tribe, has further simplified cyber-attacks. Additionally, the widespread use of social media platforms like Facebook and the popularity of mobile devices have expanded the attack surface for cyber criminals, contributing to the increasing frequency of internet-based attacks and diverse data breaches.

The motivations behind cybercrimes are notably diverse, encompassing various objectives:

- **Theft of Data:** Extending beyond financial information like credit card details and passwords, this category includes the pilfering of customer lists, intellectual property, and sensitive plans related to product development and marketing.
- **Loss of Time:** Cyber-attacks, or even the suspicion of one, can result in a significant time investment for recovery. This may involve the retrieval or reconstruction of data, along with extensive system checks.
- **Monetary Loss:** Often following data theft, financial losses are a common motivation for cybercrimes, affecting both individuals and organizations.
- **Disabled or Crippled Services:** Some cyber attackers, including protesters and certain agencies, aim to disrupt or disable targeted websites. In other cases, hackers may act with purely malicious intent.
- **Legal Exposure:** Engaging in cybercrimes, particularly those involving data or financial loss, may expose individuals or enterprises to legal repercussions. Lawsuits may be filed for the loss of entrusted data or monetary assets.

These diverse motives underscore the multifaceted nature of cyber threats, ranging from financial gain to disruptive activism and legal consequences.

In 2012, global data breaches demonstrated a varied pattern, with financial organizations constituting 37% of incidents, retail environments and restaurants at 24%, manufacturing, transportation, and utilities at 20%, and information and professional services firms also at 20%. Cyber criminals employed diverse tactics such as hacking, stolen credentials, Malware installations, physical attacks, etc., to execute these breaches. According to Verizon's 2013 annual report, 52% of breaches in 2012 involved some form of hacking, 76% exploited weak or stolen credentials, 40% utilized Malware, 35% included physical attacks, 29% relied on social tactics, and 13% resulted from privilege misuse and abuse.

Understanding the motivation behind these cyber attacks is crucial for assessing risks and determining the appropriate defences needed to protect critical resources. The multifaceted attack vectors employed underscore the importance of a comprehensive and adaptive approach to cybersecurity.

3. Descriptions of various threats of their motivations are given as follows:

Advanced Persistent Threats (APTs) or targeted attacks represent the most sophisticated and enduring cyber threats, strategically aiming at specific predetermined objectives. They often elude traditional security systems, posing risks to governments, enterprises, small businesses, and even personal networks. A survey by the Ponemon Institute revealed that 83% of IT and security practitioners believed their organizations had been targeted by advanced threats. Notable APTs include Operation Aurora and Operation Shady Remote Access Trojan (RAT).

In APT attacks, the initial step involves thorough reconnaissance to gather intelligence on the target system. Subsequently, attackers establish an initial intrusion into the target's network, creating a back door for persistent access. This is achieved by infecting a host with a bot, enabling discrete communication with the infected host. The attacker then aims to expand network access, compromising additional nodes. Once within the target, the attacker can exploit the infected host to remotely collect data or cause damage without detection. APTs are characterized by their highly personalized, targeted nature and are typically driven by strong motivation.

Motives behind APTs include:

- **Stealing Trade Secrets or Government Information:** Aiming for a competitive advantage, espionage, or warfare.
- **Infiltrating and Controlling Critical Systems:** Targeting essential infrastructure for strategic control.
- **Making Political Statements:** Hacktivists may conduct APTs to express political stances through actions like Distributed Denial of Service (DDoS) attacks or data theft.
- **Unauthorized Financial Transactions:** Involving activities such as unauthorized bank and credit card transactions.
- **Advance Fees Scams:** Engaging in schemes like the Nigerian scam, requesting money to facilitate the transfer of supposed "unclaimed" funds.
- **Product Sales from Scareware and Web-Based Enticements:** Leveraging deceptive tactics to sell fraudulent products through scareware and enticing online offers.

Highly sophisticated malware tailored for Advanced Persistent Threats (APTs) includes Stuxnet, Duqu, Flame, and Red October (Virvilis & Gritzalis, 2013). These threats have demonstrated significant capabilities, with Stuxnet notably slowing down Iran's nuclear program for four years, while others operated stealthily, extracting vast amounts of information from sensitive environments. Several recent cyber-attack incidents highlight the diverse nature of these threats:

- **South African Postbank Scam (2012):** Cybercriminals stole approximately \$6.7 million from South African Postbank over three days, using meticulously planned attacks with stolen login details to transfer funds into multiple bank accounts across the country.
- **Police Virus Scam (2012):** A major threat in 2012 involved malware infecting hundreds of thousands of computers globally, using fear and blackmailing techniques to extort money from users.

However, not all data leakage is malicious; it can also occur unintentionally due to well-intentioned employees. Instances include sending classified documents to the wrong recipients, sharing sensitive documents on public sites, or sending work files to unauthorized email accounts. Such actions can lead to brand damage, compliance violations, revenue loss, or hefty fines.

4. Instances of insider attacks also occurred:

- In April 2012, Texas A&M University unintentionally disclosed 4000 former students' sensitive information through an email attachment.
- In October 2012, Stoke-on-Trent City Council in the UK was fined £120,000 for sending emails with sensitive information to the wrong address due to a typing mistake.
- Japan's Yomiuri Shimbun fired a reporter in October 2012 for accidentally sending investigative information to the wrong recipients, compromising source identities.

Employee misuse and abuse further contribute to cybersecurity challenges, especially with the prevalence of Facebook and the use of employee-owned smartphones and tablets at work. The rise in Bring Your Own Device (BYOD) environments complicates IT administrators' efforts to secure every new device entering the network. With over 900 million Facebook users and approximately 75% of companies permitting employee-owned devices, managing and securing these devices remains an ongoing challenge.

Fully Automated Attacks:

Traditional automated attacks, such as "drive-by" attacks involving viruses and worms, have shown a decreasing trend in recent years. These attacks are initiated by the attacker, hoping that the malware will spread automatically with minimal management. The primary motivation for these attacks is often not financial gain but rather notoriety, akin to defacing a public structure. Automated attacks are relatively easy to defend against as they are indiscriminate, noisy, and can be detected with conventional security technologies. Examples of traditional worms include SQL Slammer, which congested servers and disrupted the internet without specific targeted goals.

5. Social Networking and Other Vulnerabilities:

The growing use of social media introduces significant security threats to companies and institutions. It becomes challenging to prevent employees from unintentionally disclosing sensitive company information on platforms like Facebook, Twitter, or online forums. Even seemingly harmless statements, like sharing a surprise for the boss's birthday, can offer valuable information to hackers. Recent trends indicate a shift from regular emails to social networks as preferred channels for malware distribution. In an August 2012 incident, hackers utilized Twitter and Facebook to distribute malware through social engineering techniques. For instance, a compromised Twitter account sent a misleading message to all followers, redirecting them to a malicious Facebook app under the guise of a film link. The login screen harvested Twitter credentials, enabling the hacker to repeat the process and gain access to more accounts. Stolen credentials could be exploited not only for social media but also for accessing other services like Gmail, Facebook, or even more critical accounts such as bank or business-related services. This highlights the evolving threat landscape where social engineering and the exploitation of human vulnerabilities play a crucial role in cyber attacks.

6. User-Involved Attacks:

Most security breaches involve innocent computer users, and several methods are commonly exploited:

- **Email:** Malicious attachments or links in emails, often part of phishing campaigns, serve as the primary vector for compromising computers with internet access. Social engineering tricks are employed to lure victims to infected sites, with campaigns often tailored to specific industries.
- **Web:** Attackers exploit client-side vulnerabilities when users visit infected websites, compromising client software with just a visit.
- **Instant Messaging (IM):** IM programs provide mechanisms for passing executable programs and web links, offering a means to infect computers and extract information.
- **Peer-to-Peer (P2P):** P2P environments, commonly used for sharing software, can be infiltrated with infected files.
- **Gaming:** Social interactions within gaming platforms may lead to email or IM communications that pose security risks.
- **Software Updates:** Malicious parties may exploit the updating process employed by software vendors over the internet, substituting their own software or infecting updates before they are downloaded.

DoS Attacks: Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks, although well-known, remain effective methods for disrupting IP networks. The aim is to partially or completely restrict access for legitimate users to resources provided by a victim's network, computer, or service.

DoS Attacks: Initiated from a single host, these attacks aim to restrict or deny access to a network, service, or application for legitimate users. They can be mounted successfully with limited resources but often involve flooding the victim's network with an overwhelming amount of attack packets.

DDoS Attacks: Typically involve a group of malicious hosts working together to flood the victim's network, causing a more significant impact on the performance of IP networks or services. DDoS attacks are particularly effective in disrupting or prohibiting access for legitimate users.

7. Emerging Patterns in Cybersecurity:

Recent Historical Context:

Recent times have witnessed a surge in cybersecurity challenges—record-breaking Trojan counts in malware, social network attacks, and the pervasive presence of cybercrime and cyber warfare. As we reflect on these events, it prompts us to consider what lies ahead.

Current Cyber Threat Landscape:

In the contemporary context, the term "cyber threat" is no longer a speculative concern but a daily reality. These threats are not diminishing; on the contrary, they are on an upward trajectory. Understanding these threats becomes imperative, aligning with the fundamental tenets of information security: confidentiality, integrity, and availability (Kumar et al., 2010a). A comprehensive comprehension of the motivations driving diverse cyber-attacks is crucial for projecting the forthcoming trends in this evolving landscape.

The cyber attacks can be classified into four broad categories given below:

a) Cybercrime:

In the near future, cyber crimes will prominently feature terms like cyber fraud, theft, phishing, and various malicious behaviours. Broadly, these crimes encompass malevolent activities aimed at obstructing, accessing, or interfering with cyber services. Multiple tenets of information security, including confidentiality, integrity, and availability, may be compromised during such cyber attacks. The motivations driving cyber criminals include economic gain, compromising cyber infrastructure (as seen in cyber warfare scenarios), and personal satisfaction.

Cyber criminals employ diverse attack vectors such as stolen identities, online extortion, spamming, and phishing to execute their malicious activities. The majority of real-world cyber crimes unfold through online computers, with the primary objective of gaining access to victims' computers, online resources, and credentials. Once access is obtained, compromised resources become tools for various malicious endeavors. For instance, the thriving e-commerce and online business sector become attractive targets for cyber criminals. Malware tools are frequently utilized to commit economic crimes, including the theft of credit cards, social security numbers, and electronic currency. Vulnerabilities in software used for e-commerce and online services present ample opportunities for cyber crimes in the economic domain.

Cyber crimes persist on a daily basis in the real world and are expected to persist due to the significant profits involved and the ready availability of cyber tools for committing these crimes.

b) Cyber espionage:

Cyber espionage is a clandestine operation centered on the theft of information, orchestrated by adept cyber criminals seeking access to computer systems or networks. In this realm, criminals aim to disrupt the confidentiality and integrity of system information. Their approach often involves prolonged efforts to clandestinely control or access systems, navigating through online information and circumventing existing security protocols. These criminals are typically highly skilled individuals, making detection challenging. The attack vectors in this category are intricate, often involving methods such as targeting organization employees, deploying specialized Malware, and exploiting Bring Your Own Device (BYOD) policies.

c) Key Methods of Cyber Espionage:

- **Advanced Persistent Threats (APTs):** Recent trends indicate a prevalence of highly targeted, motivated attackers, often utilizing Advanced Persistent Threats (APTs). These sophisticated attacks are expected to persist in the future, representing a significant threat landscape.
- **Malware Proliferation:** Over the past two decades, the proliferation of Malware has reached staggering levels. The numbers are astronomical, with tens of thousands of new Malware strains emerging daily. Despite enhanced preparedness among security forces, the limitless nature of the internet hampers their efforts. Cyber criminals exploit the absence of borders, allowing them to operate globally with ease. This challenges law enforcement, as cyber criminals can launch attacks from one country, steal data from another, transmit the stolen data to a server in a third country, and reside in a fourth. The speed and agility of cyber criminals contrast sharply with the time-consuming, jurisdiction-bound actions of security forces.

- **No Immunity for Companies:** Reports from security experts emphasize that no company is immune to cyber espionage attacks (Hilbert, 2013). Given the interconnected nature of business interactions, sensitive information is invariably shared, necessitating robust protection against cyber espionage threats.
- **Cyber warfare:** Cyber warfare is strategically designed to incapacitate or annihilate computer systems, typically executed through cyber weapons—specially crafted programs aimed at system targets. These attacks primarily disrupt the availability and/or integrity of the targeted systems. The motivations behind such attacks are diverse, involving government entities, military forces, or technically proficient individuals seeking recognition on a global scale.

d) Key Aspects of Cyber Warfare:

- **Targeted Disruption:** Cyber warfare employs cyber weapons to specifically target and disrupt computer systems. The primary focus is on undermining the availability and integrity of the systems in question.
- **Motivations and Actors:** The motives behind cyber warfare vary, with involvement from governments, military organizations, and technically adept individuals aspiring for global recognition. The spectrum of actors engaging in these activities is broad and continues to evolve.
- **Software Vulnerabilities:** Consistent with historical patterns, software vulnerabilities remain a prime target for cyber criminals. This method, favored by both cyber criminals and intelligence agencies globally, involves exploiting vulnerabilities to compromise systems. In 2012, Java and Adobe applications were recurrently compromised, demonstrating the prevalence of this approach.
- **Complexity of Updating:** The challenge lies in the complexity of updating applications, especially in corporate environments where coordination is essential. Slow update processes in companies create windows of opportunity for cyber attacks, both on a mass scale and in targeted forms seeking confidential data.
- **Notable Incidents:** Several high-profile incidents exemplify cyber warfare, ranging from the Russian invasion of Georgia in 2008 to the deployment of Stuxnet in 2010, which disrupted Iranian nuclear enrichment—a landmark case of a cyber network attack causing physical damage internationally. Other instances include Duqu (2011), Flame (2012), GhostNet's hacking of Tibetan exiles, and shadow networks constituting an international cyber espionage ring (Shakarian, Shakarian, & Ruef, 2013).

Today, cyber warfare has ascended to the forefront of national agendas, reflecting its profound impact on geopolitical landscapes.

8. Cyber activism:

Cyber activism emerges as a contemporary form of cybercrime, utilizing internet-based socialization and communication techniques to establish, operate, and oversee activism across diverse causes. Leveraging social networking tools and platforms such as Twitter, Facebook, LinkedIn, YouTube, and various online collaboration tools, e-activists engage in disseminating slogans, messages, and fostering interactions with netizens.

Key Aspects of Cyber Activism

- **Social Networking Tools:** Cyber activism harnesses the power of social networking tools and platforms, including Twitter, Facebook, LinkedIn, YouTube, and other specialized networks, along with email, instant messaging (IM), and other online collaboration tools. These mediums serve as conduits for sharing information and interacting with a broad audience.
- **Social Engineering Techniques:** E-activists employ social engineering techniques to share information, often tricking users into collaborating, infecting their computers, and pilfering data. The absence of security applications to safeguard users from self-compromise poses a significant challenge.
- **Targeting Social Networks:** Social networks, with their vast user base exchanging information and personal data, become prime hunting grounds for tricking users. Platforms like Facebook, Twitter, etc., attract attention, and the transition from Messenger to Skype introduces new considerations for cybersecurity.
- **Diverse Objectives:** Depending on the cause or agenda of the e-activist, cyber activism serves various purposes, including raising awareness, mobilizing followers, and initiating reactions. E-activists may utilize digital petitions, digitally signed by followers, to convey messages to government and legislative authorities.
- **Malicious Uses:** Malicious users and technically proficient individuals leverage cyber activism for more nefarious purposes. This may involve protesting against companies, executing Distributed Denial of Service (DoS) attacks by redirecting massive traffic to company websites, overwhelming servers with requests to induce failures, extracting personal information of company administrators for embarrassment, and accessing company policies to tarnish its reputation.

9. Compromised Information Integrity:

In the realm of cyber activism, the integrity of information is often compromised. Attacks may involve extracting, manipulating, or exposing sensitive information to achieve the activist's objectives (Hilbert, 2013).

Recommendations:

Holistic Network Security: Adopt a multi-layered approach to network security, moving beyond traditional tools like anti-virus and anti-phishing. Understand the motivations behind attacks and tailor defences accordingly.

Integrated Security Measures: Integrate various security layers such as intrusion prevention, protocol and behaviour analysis, application control, and vulnerability management to identify and isolate threats effectively. Ensure all protection layers are enabled for maximum effectiveness.

Best Practices Implementation: Implement best practices to raise the bar on attacker and limit the impact of malware. Consider architecture and detection techniques for Intrusion Detection Systems (IDSs), employing feature selection technique and AI-based methods to enhance real-time capabilities.

Data Loss Prevention (DLP): Implement automated corporate policies, specifically DLP solutions, to catch incidents of data loss before it leaves the organization. Develop a clear DLP strategy, defining confidential information and user permissions.

Security Policy and User Education: Define and enforce a comprehensive security policy that guides secure operations. Involve users in security measures through training, making them aware of cyber threats, security policies, and their role in preventing attacks.

10. Conclusion:

In the face of evolving cyber threats, robust protection is crucial. Emphasize a strong security policy, regular updates to security products, user education, and common-sense practices. The growing number of threats underscores the importance of a proactive and integrated approach to cybersecurity. Additionally, positive strides in global cooperation among law enforcement, such as Interpol's plan for a "Global Cybercrime Center," provide hope in the ongoing fight against cybercrime.