TECH CHRONICLE 2021

A WEBZINE
OF THE DEPARTMENT OF
COMPUTER SCIENCE
VIVEKANANDA MISSION
MAHAVIDYALAYA

Tech Chronicle, Vol-1, Issue-1,
A webzine of the Department of Computer Science,
Published in December, 2021

Published by:
Principal,
Vivekananda Mission Mahavidyalaya

Conception and Planning:

Department of Computer Science,
Vivekananda Mission Mahavidyalaya

Editor:
Mr. Debajit Sensarma,
Assistant Professor,
Department of Computer Science

Principal’s Message

I am glad to know that the department of Computer Science is bringing out the webzine **Tech Chronicle**. It's a very good initiative to represent spontaneous outburst of many hidden talents through this online magazine in this covid 19 global pandemic situation.

I convey my heartiest greetings & best wishes to all staffs and students for their coordination and efforts. I wish it's grand success.

Dr. Manabendra Sahu,
Principal,
Vivekananda Mission Mahavidyalaya

Head of the Department's Column

In a world driven by rapid technological advancements, staying informed, reflective, and connected has become more important than ever. It is with great pride and excitement that I introduce our department's new webzine, **Tech Chronicle**, a platform born out of our collective passion for innovation and our commitment to shaping the future of technology.

Tech Chronicles is not just a publication; it is a celebration of curiosity, creativity, and collaboration. It represents a confluence of ideas and insights, offering a window into the dynamic world of technology and its profound impact on our lives.

Through this webzine, we aim to achieve three primary objectives:

1. **Encourage Exploration**: Technology is vast and ever-evolving, often overwhelming in its complexity. *Tech Chronicles* strives to make these advancements accessible by presenting articles, interviews, and stories that both inform and intrigue. From artificial intelligence to sustainability in tech, our content is designed to spark curiosity and encourage exploration.
2. **Foster Engagement**: One of the unique aspects of *Tech Chronicles* is its inclusive approach. It serves as a platform where students, faculty, researchers, and industry experts can share their insights and perspectives. This interactive space is a reflection of our belief that learning is a shared journey.
3. **Inspire Action**: Innovation is not merely about understanding technology—it's about leveraging it to create meaningful change. Whether it's highlighting groundbreaking research or celebrating small yet impactful

innovations, *Tech Chronicles* aims to inspire readers to take action and contribute to shaping a better future.

I would like to take this opportunity to commend the editorial team for their vision, dedication, and hard work in bringing this project to life. They have meticulously curated content that reflects the dynamism and diversity of our department and the tech world at large.

As we embark on this exciting journey, I encourage all of you—our students, faculty, alumni, and readers—to actively engage with *Tech Chronicles*. Your contributions, feedback, and ideas will be instrumental in enriching this platform and ensuring its growth as a vibrant hub of knowledge and innovation.

Let *Tech Chronicles* serve as a beacon for creativity and exploration, a testament to our department's commitment to excellence, and a source of pride for our community. Together, let us chart the path forward, embracing the challenges and opportunities that technology presents.

Thank you for your support, and I look forward to seeing *Tech Chronicles* evolve into a powerful voice in the ever-changing narrative of technology.

Warm regards,

Mr. Debajit Sensarma,

Head of the Department,

Department of Computer Science

From the Editor's Desk

Welcome to **Tech Chronicles**, your gateway to the ever-evolving world of technology. In an age defined by rapid innovation, our mission is simple: to decode the complexities of technology and present them in a way that informs, inspires, and empowers.

At **Tech Chronicle**, we explore the cutting-edge advancements shaping our world—from artificial intelligence and blockchain to renewable energy and space exploration. Our stories are not just about the "what" of technology but also the "why" and "how," delving into the ethical, social, and economic impacts of innovation.

Our webzine is a space where ideas thrive, and diverse perspectives converge. You'll find in-depth analyses, thought-provoking opinion pieces, hands-on reviews, and stories that spotlight ground-breaking start-ups and industry leaders alike. Whether you are a tech enthusiast, a professional navigating the digital landscape, or simply curious about what the future holds, there is something here for you.

As we chronicle the pulse of technology, we invite you to join the conversation. Share your thoughts, challenge perspectives, and suggest topics you'd like to see explored. Together, let's navigate this thrilling journey into the future.

Thank you for being a part of our community.

Mr. Debajit Sensarma,

Assistant Professor,

Department of Computer Science,

Vivekananda Mission Mahavidyalaya

Table of Contents

CYBER-SECURITY

By Malay Maity
3rd Sem, Department of Computer Science

ABSTRACT:
Cyber Security plays an important role in the field of information technology. Securing the information have become one of the biggest challenges in the present day. Whenever we think about the cyber security the first thing that comes to our mind is 'cyber crimes' which are increasing immensely day by day. Various Governments and companies are taking many measures in order to prevent these cyber-crimes. Besides various measures cyber security is still a very big concern to many.

Introduction:

Cyber security is the most concerned matter as cyber threats and attacks are overgrowing. Attackers are now using more sophisticated techniques to target the systems. Individuals, small-scale businesses or large organization, are all being impacted. So, all these firms whether IT or non-IT firms have understood the importance of Cyber Security and focusing on adopting all possible measures to deal with cyber threats.

What is cyber-security:

Cyber security is the protection of Internet-connected systems, including hardware, software, and data from cyber attacks. It is made up of two words one is cyber and other is security.

- Cyber is related to the technology which contains systems, network and programs or data.
- Whereas security related to the protection which includes systems security, network security and application and information security

WHY DO WE NEED CYBER SECURITY?

The range of operations of cyber security involves protecting data and systems from cyber threats. These threats can be many forms. As a result, keeping pace with cyber security strategy and operations can be a more challenges, particularly in government and enterprise networks & data center. Some of more reasons are: -

- Cyber-attacks can be extremely expensive for businesses to endure.

- In addition to financial damage suffered by the business, a data breach can also inflict untold reputational damage. • Cyber-attacks these days are becoming progressively destructive. Cybercriminals are using more sophisticated ways to initiate cyber-attacks.

- Regulations such as GDPR are forcing organizations into taking better care of the personal data they hold. Because of the above reasons, cyber security has become an important part of the business and the focus now is on developing appropriate response plans that minimize the damage in the event of a cyber-attack. But an organization or an individual can develop a proper response plan only when he has a good grip on cyber security fundamentals.

Cyber security Fundamentals

1. ***Confidentiality:*** Confidentiality, is all about to prevent data from unofficially access from parities i.e., hiding data from random accessing;

   Standard measure to build a strong confidentiality include:

   - ✓ **Data Encryption.**
   - ✓ **Bio-metric Authentication (such as finger print, Corina).**
   - ✓ **Two-step verification.**
   - ✓ **Security Tokens.**

2. ***Integrity:*** Integrity, is all about to prevent data form modification from unauthorize parties.

   Standard integrity services must include:

   - ✓ **Cryptography checksums.**
   - ✓ **File protection.**
   - ✓ **Continuous power supply.**
   - ✓ **Data backup.**
   - ✓ **Access protection.**

3. ***Availability:*** Avability is to make sure of data accessing according to need .

   Most of Standard availability include: -

   - ✓ **Continuous power supply.**
   - ✓ **Backup data in external drives.**
   - ✓ **Data redundancy.**

<<>> Types of Cyber-attacks >>

A cyber-attack is an exploitation of computer systems and networks. It uses malicious code to alter computer code, logic or data and lead to cybercrimes, such as information and identity theft.

Based on type cyber-attacks may classified into two category –

1.Web-based attacks :>>

Basically web-based attack only occurs in website. Some of web-based attacks are ->

- ***URL Interpretation >*** It is a type of attack where we can change the certain parts of a URL, and one can make a web server to deliver web pages for which he is not authorized to browse.

- ***Injection attacks >*** In injection attack some data will be injected into a web application to manipulate the application and fetch the required information.
  Ex -> SQL Injection, code Injection, log Injection, XML Injection etc.

- ***DNS Spoofing >*** DNS Spoofing is a type of computer security hacking where a data is introduced into a DNS resolver's cache causing the name server to return an incorrect IP address, diverting traffic to the attacker's computer or any other computer. The DNS spoofing attacks can go on for a long period of time without being detected and can cause serious security issues.

- ***Session Hijacking >*** Attacking on a user session over a protected network called session hijacking. Any web applications make cookies to store the state and user sessions for providing enhanced service but by stealing the it any how, an attacker can have access to all of the user data.

- ***Phishing >*** Phishing is a type of attack which attempts to steal sensitive information like user login credentials and credit card number. It occurs when an attacker is masquerading as a trustworthy entity in electronic communication.

- ***Brute force >*** It is a type of attack which uses a trial-and-error method. This attack generates a large number of guesses and validates them to obtain actual data like user password and personal identification number. This attack may be used by criminals to crack encrypted data, or by security, analysts to test an organization's network security.

- ***Denial oof services >*** It is an attack which meant to make a server or network resource unavailable to the users. It accomplishes this by flooding the target with traffic or sending it information that triggers a crash. It uses the single system and single internet connection to attack a server. It can be classified into the following-

  - ***Volume-based attacks- >*** Its goal is to saturate the bandwidth of the attacked site, and is measured in bit per second.
  - ***Protocol attacks->*** It consumes actual server resources, and is measured in a packet.
  - ***Application layer attacks->*** Its goal is to crash the web server and is measured in request per second.

- ***Directory attack >*** This type of attack stored the list of a commonly used password and validated them to get original password.

- ***File Inclusion attack >*** File inclusion allows an attacker to access unauthorized or essential files which is available on the web server or to execute malicious files on the web server by making use of the include functionality.

- ***Man in the middle attack >*** In man-in-middle attack ,an attacker to intercepts the connection between client and server and acts as a bridge between them. Due to this, an attacker will be able to read, insert and modify the data in the intercepted connection.

2.System based attack :>> These are the attacks which are intended to compromise a computer or a computer network. Some of the important system-based attacks are as follows >>

- ***Virus >*** A virus is a program that attempts to damage a computer system and replicate itself to other computer systems. A virus usually attaches to files with execution capabilities such as .doc, .exe, and .bat extensions.
  Ex -> Stoned, Melissa.

- ***Worm >*** A worm is a self-replicating program that can be designed to do any number of things, such as delete files or send documents via e-mail. A worm can negatively impact network traffic just in the process of replicating itself. Worms often originate from email attachments that appear to be from trusted senders.
  Ex -> Code Red.

- ***Trojan horse >*** A Trojan horse is a malicious program that is disguised as legitimate software that occurs unexpected changes to computer setting and unusual activity, even when the computer should be idle. It misleads the user of its true intent. It appears to be a normal application but when opened/executed some malicious code will run in the background.
  Ex ->Back Orifice, Net Bus.

- ***Backdoors >*** It is a method that bypasses the normal authentication process. A developer may create a backdoor so that an application or operating system can be accessed for troubleshooting or other purposes.

- ***Bots >*** A bot (short for "robot") is an automated process that interacts with other network services. Some bots program run automatically, while others only execute commands when they receive specific input. Common examples of bots' program are the crawler, chatroom bots, and malicious bots.

- ***What is a threat:*** A threat is any incident that could negatively affect an asset – for example, if it's lost, knocked offline or accessed by an unauthorized party. Threats can be categorized as circumstances that compromise the confidentiality, integrity or availability of an asset, and can either be intentional or accidental. Intentional threats include things such as criminal hacking or a malicious insider stealing information, whereas accidental threats generally involve employee error, a technical malfunction or an event that causes physical damage, such as a fire or natural disaster.

- ***Cyber Warfare:*** Cyber warfare refers to the use of digital attacks -- like computer viruses and hacking -- by one country to disrupt the vital computer systems of another, with the aim of creating damage, death and destruction. Future wars will see hackers using computer code to attack an enemy's infrastructure, fighting alongside troops using conventional weapons like guns and missiles. Cyber warfare involves the actions by a nation-state or international organization to attack and attempt to damage another nation's computers or information networks through, for example, computer viruses or denial-of-service attacks.

- ***Cyber Crime:*** Cybercrime is criminal activity that either targets or uses a computer, a computer network or a networked device. Cybercrime is committed by cybercriminals or hackers who want to make money. Cybercrime is carried out by individuals or organizations. Some cybercriminals are organized, use advanced techniques and are highly technically skilled. Others are novice hackers.

- ***Cyber terrorism: >*** It is the most innovative use of information technology by terrorist groups to further their agenda. Terrorism in the form of attacks on official networks (governmental, non-governmental), banking server and telecommunication infrastructures.

- ***Cyber Espionage: >*** Cyber spying, or cyber espionage, is the act or practice of obtaining secrets and information without the permission and knowledge of the holder of the information from individuals, competitors, rivals, groups, governments and enemies for personal, economic, political or military advantage using methods on the Internet.

Who are Cyber Criminals?

Cyber-criminals are those who can't done anything physically but by using IT, operate their evil job. Such as finance card fraud (credit, debit…), cyber stalking, defaming through online, gaining unauthorized access to computer systems, ignoring copyright, without official likens use software and its trademark, making illegal copies break encryption; software piracy and stealing identity to perform criminal acts. They can be categorized into three groups that reflect their motivation: -

❖ ***Type 1: Cybercriminals – hungry for recognition:***
- ✓ Hobby hackers;
- ✓ IT professionals (social engineering is one of the biggest threats);
- ✓ Politically motivated hackers;
- ✓ Terrorist organizations.

❖ ***Type 2: Cybercriminals – not interested in recognition***:
- ✓ Psychological prevents;
- ✓ Financially motivated hackers (corporate espionage);
- ✓ State – sponsored hacking (national espionage, sabotage);
- ✓ Organized criminals.

❖ ***Type 3: Cybercriminals – the insiders:***
- ✓ former employees seeking revenge;
- ✓ Competing companies using employees to gain economic advantage through damage and/or theft.

Trending change of cyber-security: > Here is the day where we all are more and more dependent on internet, as well as there a huge revolutionary change on internet like –

❖ **Web server:** Cyber criminals distribute their malicious code via legitimate web servers they've compromised. But data-stealing attacks, many of which get the attention of media, are also a big threat. Now, we need a greater emphasis on protecting web servers and web applications. Web servers are especially the best platform for these cyber criminals to steal the data. Hence one must always use a safer browser especially during important transactions in order not to fall as a prey for these crimes.

❖ **Cloud computing:** These days, the world is slowly moving towards the clouds. This latest trend presents a big challenge for cyber security. Additionally, as the number of applications available in the cloud grows, policy controls for web applications and cloud services will also need to evolve in order to prevent the loss of valuable information. Cloud may provide immense opportunities but it should always be noted that as the cloud evolves so as its security concerns increase.

❖ **Code encryption:** Encryption is the process of encoding of information in such a way that any un authorized partis cannot access it randomly. In an encryption scheme, the message or information is encrypted using an encryption algorithm, turning it into an unreadable cipher text. Encryption at a very beginning level protects data privacy and its integrity. But more use of encryption brings more challenges in cyber security. Encryption is also used to protect data in transit, for example data being transferred via networks (e.g., the Internet, e-commerce), mobile telephones, wireless microphones, wireless intercoms etc.

❖ **Advanced Persistent Threat (APT):** APT is a wholly new level of cybercrime ware. For years network security capabilities such as web filtering or IPS have played a key part in identifying such targeted attacks (mostly after the initial compromise). As attackers grow bolder and employ more vague techniques, network security must integrate with other security services in order to detect attacks. Hence one must improve our security techniques in order to prevent more threats coming in the future.

❖ **Mobile network:** Today we are able to connect to anyone in any part of the world. But for these mobile network's security is a very big concern. These days firewalls and other security measures are becoming porous as people are using devices such as tablets, phones, PC's etc. all of which again require extra securities apart from those present in the applications used. We must always think about the security issues of these mobile networks. Further mobile networks are highly prone to these cybercrimes a lot of care must be taken in case of their security issues.

❖ **IPv6 internet protocol:** IPv6 is the new Internet protocol which is replacing IPv4 (the older version), which has been a backbone of our networks in general and the Internet at large. Protecting IPv6 is not just a question of porting IPv4 capabilities. While IPv6 is a wholesale replacement in making more IP addresses available, there are some very fundamental changes to the protocol which need to be considered in security policy. Hence it is always better to switch to IPv6 as soon as possible in order to reduce the risks regarding cyber-crime.

Security Policies:>> Security policies are a formal set of rules which is issued by an organization to ensure that the user who are authorized to access technology and information with rules and guidelines related to the security of information. A security policy also considered to be a "living document" which means that the document is never finished, but it is continuously updated as requirements of the technology. Most types of security policies are automatically created during the installation. We have to customize policies that suit our specific environment.

<: :>CYBER SECURITY TECHNIQUES

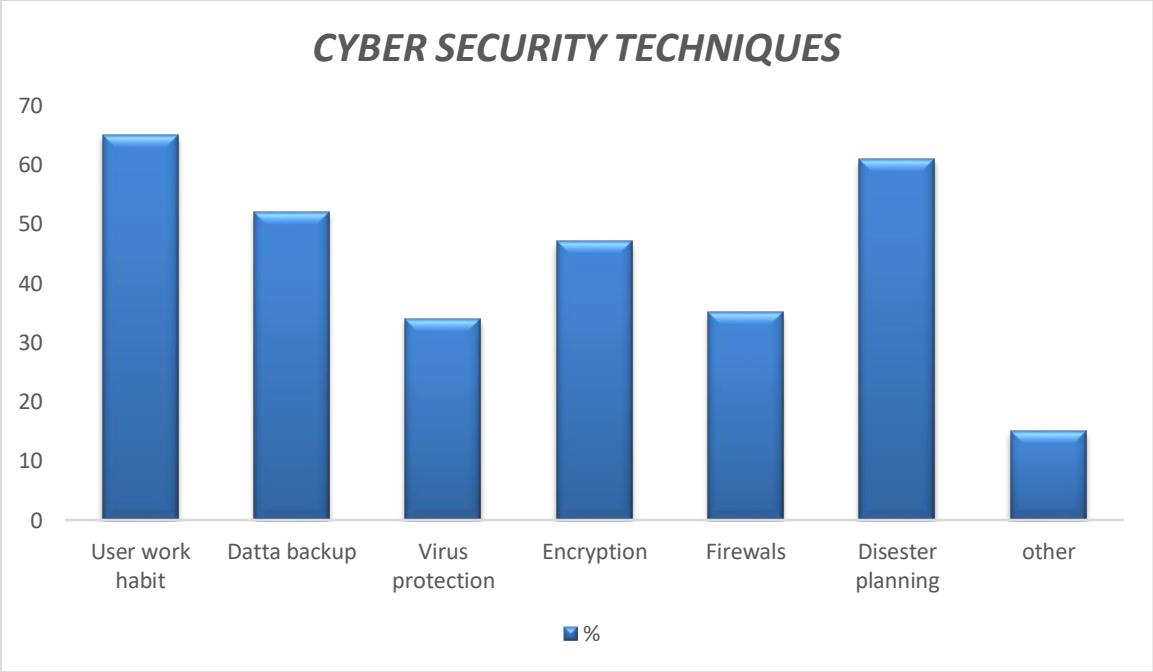
- ***Access control and password security :>*** The concept of user name and password has been fundamental way of protecting our information. This may be one of the first measures regarding cyber security.

- ***Authentication of data :>*** The documents that we receive must always be authenticated be before downloading that is it should be checked if it has originated from a trusted and a reliable source and that they are not altered. Authenticating of these documents is usually done by the anti-virus software present in the devices. Thus, a good anti-virus software is also essential to protect the devices from viruses.

- ***Malware scanners :>*** This is software that usually scans all the files and documents present in the system for malicious code or harmful viruses. Viruses, worms, and Trojan horses are examples of malicious software that are often grouped together and referred to as malware.

- ***Firewalls :>*** A firewall is a software program or piece of hardware that helps screen out hackers, viruses, and worms that try to reach your computer over the Internet. All messages entering or leaving the internet pass through the firewall present, which examines each message and blocks those that do not meet the specified security criteria. Hence firewalls play an important role in detecting the malware.

- ***Anti-virus software :>*** Antivirus software is a computer program that detects, prevents, and takes action to disarm or remove malicious software programs, such as viruses and worms. Most antivirus programs include an auto-update feature that enables the program to download profiles of new viruses so that it can check for the new viruses as soon as they are discovered. An anti-virus software is a must and basic necessity for every system.



CYBER ETHICS :> Cyber ethics are nothing but the code of the internet. When we practice these cyber ethics there are good chances of us using the internet in a proper and safer way. The below are a few of them:

- ✓ Use Strong Passwords Use different user ID / password combinations for different accounts and avoid writing them down. Make the passwords more complicated by combining letters, numbers, special characters (minimum 10 characters in total) and change them on a regular basis.

- ✓ Secure your computer o Activate your firewall Firewalls are the first line of cyber defense; they block connections to unknown or bogus sites and will keep out some types of viruses and hackers.

- ✓ Use anti-virus/malware software Prevent viruses from infecting your computer by installing and regularly updating anti-virus software. o Block spyware attacks Prevent spyware from infiltrating your computer by installing and updating anti-spyware software.

- ✓ Be Social-Media Savvy Make sure your social networking profiles (e.g., Facebook, Twitter, YouTube, etc.) are set to private. Check your security settings. Be careful what information you post online. Once it is on the Internet, it is there forever!

- ✓ Secure your Mobile Devices Be aware that your mobile device is vulnerable to viruses and hackers. Download applications from trusted sources.

- ✓ Install the latest operating system updates Keep your applications and operating system (e.g., Windows, Mac, Linux) current with the latest system updates. Turn on automatic updates to prevent potential attacks on older software.

- ✓ Protect your Data Use encryption for your most sensitive files such as tax returns or financial records, make regular back-ups of all your important data, and store it in another location.

- ✓ Secure your wireless network Wi-Fi networks at home are vulnerable to intrusion if they are not properly secured. Review and modify default settings. Public Wi-Fi, a.k.a. “Hot Spots”, are also vulnerable. Avoid conducting financial or corporate transactions on these networks.

- ✓ Protect your e-identity Be cautious when giving out personal information such as your name, address, phone number or financial information on the Internet. Make sure that websites are secure (e.g., when making online purchases) or that you’ve enabled privacy settings (e.g., when accessing/using social networking sites).

- ✓ Avoid being scammed Always think before you click on a link or file of unknown origin. Don’t feel pressured by any emails. Check the source of the message. When in doubt, verify the source. Never reply to emails that ask you to verify your information or confirm your user ID or password.

- ✓ Call the right person for help Don’t panic! If you are a victim, if you encounter illegal Internet content (e.g., child exploitation) or if you suspect a computer crime, identity theft or a commercial scam, report this to your local police. If you need help with maintenance or software installation on your computer, consult with your service provider or a certified computer technician

CONCLUSION

Computer security is a vast topic that is becoming more important because the world is becoming highly interconnected, with networks being used to carry out critical transactions. Cybercrime continues to diverge down different paths with each New Year that passes and so does the security of the information. The latest and disruptive technologies, along with the new cyber tools and threats that come to light each

Ransomware: The Digital Age Threat

Paramita Samanta,3rd Sem

In the interconnected digital world, ransomware has emerged as a significant cybersecurity threat. This malicious software, designed to encrypt or lock victims' data, is often accompanied by a demand for ransom payments in exchange for data recovery. Ransomware attacks target individuals, businesses, governments, and critical infrastructure, causing financial losses, operational disruptions, and reputational damage. Understanding the workings, impacts, and mitigation strategies of ransomware is essential in combating this escalating cyber menace.

What is Ransomware?

Ransomware is a type of malware that encrypts a victim's files or locks their system, rendering it inaccessible. Once infected, victims receive a ransom demand—typically in cryptocurrency—promising decryption keys in return for payment. The malicious software is often spread through phishing emails, malicious websites, infected software downloads, or vulnerabilities in outdated systems.

Ransomware can be broadly classified into two types:

Crypto Ransomware: Encrypts files, making them unusable until a decryption key is provided.

Locker Ransomware: Locks users out of their devices without encrypting files, often targeting mobile devices.

Prominent ransomware attacks like WannaCry and Petya have showcased the devastating potential of such threats, affecting millions worldwide.

How Ransomware Works

Infection Vector:
Ransomware typically infiltrates systems through phishing emails, malicious attachments, or exploiting software vulnerabilities.
Execution:
Once installed, the malware begins encrypting files or locking the system. Advanced strains can spread across networks, infecting multiple devices.

Ransom Note:
After encrypting data, the attacker displays a ransom note, detailing payment instructions, often with a deadline. Failure to pay may result in permanent data loss or increased ransom demands.

Optional Decryption:
Paying the ransom does not guarantee the return of data, as attackers may fail to provide a working decryption key.

Impact of Ransomware Attacks

Financial Losses:
Organizations face significant expenses, including ransom payments, data recovery costs, and operational downtime. The global cost of ransomware is projected to reach billions annually.

Data Breaches:
Some ransomware groups exfiltrate sensitive data before encryption, threatening to release it publicly if the ransom is not paid.

Disruption of Services:
Critical sectors like healthcare, energy, and transportation have been prime targets. For example, the Colonial Pipeline attack in 2021 disrupted fuel supplies across the U.S. East Coast.

Reputational Damage:

Victims often suffer a loss of trust from customers, stakeholders, and the public, further amplifying the consequences of an attack.
National Security Risks:
Ransomware attacks on infrastructure, defense, or government systems pose significant threats to national security.

Fighting Ransomware Preventive Measures:

Education: Train employees to recognize phishing attempts and avoid suspicious downloads.
System Updates: Regularly update software and operating systems to patch vulnerabilities.
Backups: Maintain regular, offline backups of critical data to ensure recovery without paying a ransom.
Technological Defenses:

Use robust antivirus software and firewalls.
Employ endpoint detection and response (EDR) tools to identify and neutralize threats in real time.

Incident Response:

Develop a ransomware response plan, including isolating infected systems to prevent the spread of malware.
Engage cybersecurity professionals for containment and recovery efforts.
Avoid Paying Ransom:
Law enforcement agencies discourage paying ransoms, as it encourages attackers and does not guarantee data recovery.

Collaboration:
Governments, cybersecurity firms, and international organizations must work together to track and dismantle ransomware groups. Operations by agencies like INTERPOL and the FBI have disrupted major ransomware gangs, reducing their reach.

Future Challenges:
The ransomware landscape continues to evolve. Attackers are adopting new tactics, such as ransomware-as-a-service (RaaS), where developers sell ransomware kits

to other criminals. Emerging technologies like artificial intelligence (AI) are also being leveraged to create more sophisticated attacks. As organizations migrate to cloud systems, ransomware groups are targeting cloud environments, posing additional challenges.

Conclusion:
Ransomware represents a critical threat in the digital age, affecting individuals and organizations across the globe. Combating ransomware requires a proactive approach, blending preventive measures, advanced technologies, and international collaboration. By fostering awareness, implementing robust defenses, and encouraging global cooperation, we can mitigate the impact of ransomware and build a safer, more resilient digital environment. As technology evolves, so must our strategies to counter this ever-present danger.

Hacking

By: **Shilpa Pradhan, B.Sc. Computer Science (3rd Sem)**
Vivekananda Mission Mahavidyalaya

The explosive growth of the Internet has brought many good things: electronic commerce, easy access to vast stores of reference material, collaborative computing, e-mail, and new avenues for advertising and information distribution, to name a few. As with most technological advances, there is also a dark side: criminal hackers.

Governments, companies, and private citizens around the world are anxious to be a part of this revolution, but they are afraid that some hacker will break into their Web Server and replace their logo with bad images, read their e-mail, steal their credit card number from an online shopping site, or implant software that will secretly transmit their organization's secrets to the open Internet. With these concerns and others, the ethical hacker can help.

History of Hacking

When hacking first started it was not thought of as that serious. The first computer hackers emerged at MIT in the 1960's. No one seemed to mind hackers back in the 1960s when this was the most widely accepted reputation. In fact, most people had no idea what hacking was. During those times, computers were mainframes, locked away in temperature controlled, glassed in areas. It cost a lot of money to run these machines, so programmers had limited access to them. The smarter students, usually MIT students, had a curiosity about how things worked. In 1969, Bell Labs employee Ken Thompson invented UNIX and permanently changed the future of the computer industry. Then in the very early 1970s, Dennis Ritchie invented the computer programming language "C" which was specifically invented to be used with UNIX. A group called the "414s" is one of the earliest hacker groups to ever get raided by the FBI and they get charged with 60 computer intrusions. Usenets began to pop up around the nation at this time and hackers exchanged thoughts using their UNIX based machines. The infamous hacker groups the "Legion of Doom," based in the USA and the "Chaos Computer Club," based in Germany, were founded and are still two of the most widely recognized and respected hacker groups ever founded. During the 1990s, Kevin Mitnick is arrested after being tracked down by Tsutomu Shimomura. The trials of Kevin Mitnick were of the most publicized hacker trials in hacker history.

What is Hacking

Hacking is the gaining of access (wanted and unwanted) to a computer and viewing, copying or creating data (leaving a trace) without the intention of destroying a data or maliciously harming the computer. One example of computer hacking is the use of a password cracking technique to gain access to a computer system. The process of gaining illegal access to a computer system, or a group of computer systems, is known as hacking.

Who is Hacker?

Person who gains authorized/unauthorized access to a computer without the intention of causing damage. In the computer security context, a hacker is someone who seeks and exploits weaknesses in a computer system or computer network. Hackers may be motivated by a multitude of reasons, such as profit, protest, challenge, enjoyment, or to evaluate those weaknesses to assist in removing them. The subculture that has evolved around hackers is often referred to as the computer underground. A hacker is any per who engaged in hacking.

Types of Hackers

Hacker are of three types: 1) Black Hat Hacker. 2) White Hat Hacker. 3)Grey Hat Hacker.

Black Hat Hacker

Black Hat hackers are the ones with poor intentions. Black hat hackers are criminals who bypass security protocols and break into computer networks. Their primary goal is to make money, but sometimes, they're involved in corporate espionage or activism. Not only do they look to steal data, but they often seek to modify or destroy it, depending on their motivations.

The best protection is to be proactive by keeping your firewall turned on, updating and running reputable antivirus software and antispyware applications, and immediately installing all operating system updates. Additionally, don't download anything from unknown sources and disconnect your computer from the internet or turn it off when you aren't using it, to reduce exposure to hackers.

White Hat Hacker

White hat hackers, also referred to as "ethical hackers," are cybersecurity specialists who test systems' security. A white hat hacker is hired to break into computer networks with the aim of finding loopholes or flaws in cybersecurity systems that other hackers could potentially misuse. White hat hackers may do their research on open-source software, as well as on software or systems they own or have been authorized to investigate, including products and services that operate bug bounty programs. white hat hackers respect the rule of law as it applies to hacking. Unlike black or grey hat hackers, white hat hackers fully disclose all the vulnerabilities they find to the company or product owner who is responsible for fixing the flaws so the issues can be resolved before they are exploited by malicious hackers.

Grey Hat Hacker

A hacker who is in between ethical and black hat hackers. He/she breaks into computer systems without authority with a view to identify weaknesses and reveal them to the system owner. These types of hackers are not inherently malicious with their intents; they're just looking to get something out of their discoveries for themselves.

Famous hackers in history

Kevin Mitnick

Kevin David Mitnick (born August 6, 1963) is an American computer security consultant, author, and convicted hacker. In the mid-nineties, he was "The World's Most Wanted Hacker". Since 2000, he has been a successful security consultant, public speaker and author. Kevin does security consulting for Fortune 500 companies, performs penetration testing services for the world's largest companies and teaches Social Engineering classes to dozens of companies and government agencies. Kevin is now "The World's Most Famous Hacker" and has been the subject of countless news and magazine articles published throughout the world. His last book 'Ghost in the Wires: My Adventures as the World's Most Wanted Hacker' was a New York Times bestseller.

Albert Gonzalez

Albert Gonzalez (born 1981) is an American computer hacker and computer criminal who is accused of masterminding the combined credit card theft and subsequent reselling of more than 170 million card and ATM numbers from 2005 to 2007: the biggest such fraud in history. On March 25, 2010, Gonzalez was sentenced to 20 years in federal prison. Gonzalez, along with his team, were featured on the 5th-season episode of the CNBC series American Greed titled: "Episode 40: Hackers: Operation Get Rich or Die Tryin".

Michael Calce

Michael Calce, formerly known as "MafiaBoy," it was notoriety. In 2000, at 15 years old, he executed a massive denial-of-service (DoS) attack that crippled some of the internet's most popular websites. Calling the attack Rivolta, meaning "riot" in Italian, he brought down Yahoo!, eBay, CNN, Amazon, and other sites, causing an estimated $1.7 billion in damages.

Kevin Poulsen

Kevin Poulsen is a former computer hacker, whose best-known hack involved penetrating telephone company computers in the early 1990s to win radio station phone-in contests. By taking over all the phone lines leading to Los Angeles radio stations, he was able to guarantee that he would be the proper-numbered caller to win, for example, $20,000 in cash, and a Porsche 944 S2 Cabriolet.

Adrián Lamo

Adrián Alfonso Lamo Atwood (February 20, 1981 – March 14, 2018) was an American threat analyst and hacker. Adrián Lamo, a hacker best known for breaking into the computer networks of The New York Times and other major corporations, and for reporting the Army whistle-blower Chelsea Manning to the authorities.

Types of Hacking

Ethical Hacking

Ethical hacking is a process of detecting vulnerabilities in an application, system, or organization's infrastructure that an attacker can use to exploit an individual or organization. They use this process to prevent cyberattacks and security breaches by lawfully hacking into the systems and looking for weak points.

Website Hacking

Hacking a website means taking control from the website owner to a person who hacks the website.

Network Hacking

Network Hacking is generally means gathering information about domain by using tools like Telnet, Ns look UP, Ping, Tracert, Netstat, etc... over the network.

Email Hacking

Email Hacking is another form of man-in-the-middle attack, in which the hacker compromises and gain access to a target's email account. The attacker then silently monitors the communications between the client and the provider and uses the information for malicious purposes.

Password Hacking

Password Hacking Password cracking is the process of recovering secret passwords from data that has been stored in or transmitted by a computer system.

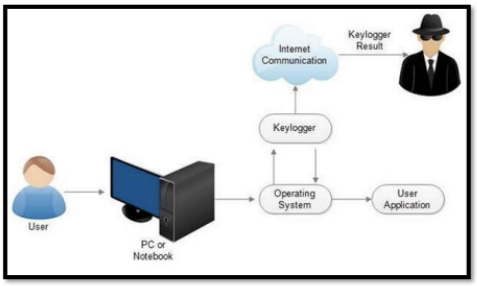
Online Banking Hacking

Online banking Hacking Unauthorized accessing bank accounts without knowing the password or without permission of account holder is known as Online banking hacking.

Computer Hacking

Computer Hacking is when files on your computer are viewed, created, or edited without your authorization.

Hacking Techniques



KEYLOGGER

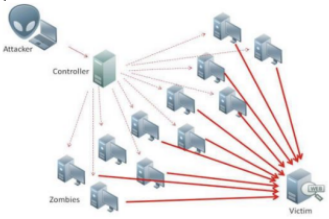
Keyloggers are many hackers and script kiddie's favourite tools. Keylogging is a method that was first imagined back in the year 1983.

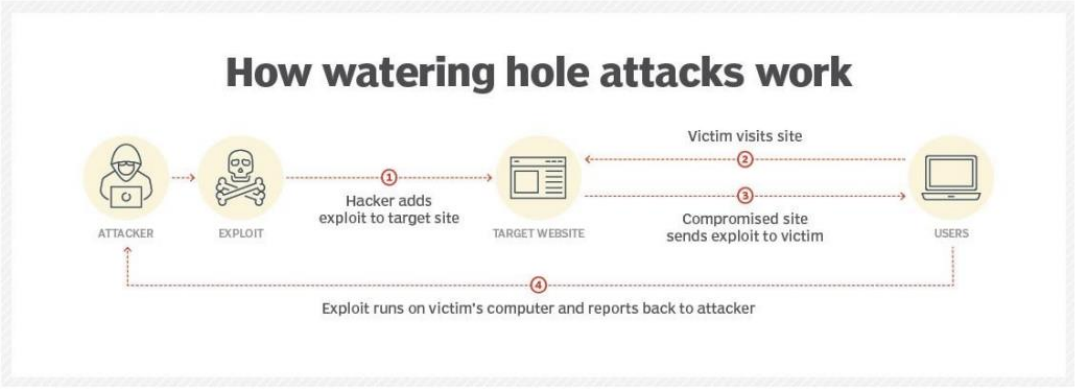
keylogger is a simple software that records the key sequence and strokes of your keyboard into a log file on your machine. these log files might even contain your personal email ids and passwords.

keylogger is one of the main reasons why online banking sites give you an option to use their virtual keyboards.

DENIAL OF SERVICE ATTACK

A Denial-of-service attack is hacking technique to take down a site or server by flooding that site or server with a lot of traffic that the server is unable to process all the requests in the real time and finally crashes down. Distributed denial of service attacks may be the most well-known type of hacking incident – the 2018 GitHub and 2016 Dyn DDoS attacks being the most prominent – but there are many other kinds of denial-of-service attacks that don't necessarily involve the distributed or botnet approach for DDOS attacks, hackers often deploy botnets or zombie computers which have got the only work to flood your system with request packets.





WATERHOLE ATTACKS

The term watering hole attack comes from hunting. Rather than tracking its prey over a long distance, the hunter instead determines where the prey is likely to go, most commonly to a body of water the watering hole and the hunter waits there. When the prey comes of its own will, often with its guard down, the hunter attacks.

The target victim can be an individual, an organization or a group of people. The attacker profiles its targets typically, employees of large enterprises, human rights organizations, religious groups or government offices to determine the type of websites they frequent. These are often messaging boards or general interest sites popular with the intended target.

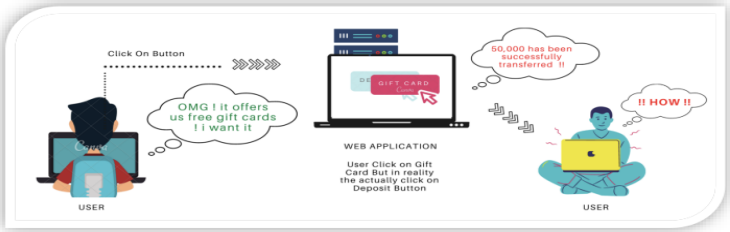
Watering hole attacks a type of social engineering attack are also referred to as water-holing, a water hole attack or a strategically compromised website.

EAVESDROPPING

An eavesdropping attack occurs when a hacker intercepts, deletes, or modifies data that is transmitted between two devices. Eavesdropping, also known as sniffing or snooping, relies on unsecured network communications to access data in transit between devices. Through these attacks, your information like passwords, card details, and other sensitive data is easily stolen while it is getting transferred from one device to another.

The motive behind eavesdropping is not to harm the system but to get some information without being identified.

CLICKJACKING



Typically, clickjacking is performed by displaying an invisible page or HTML element, inside an iframe, on top of the page the user sees. The user believes they are clicking the visible page but in fact they are clicking an invisible element in the additional page transposed on top of it.

Clickjacking attacks attempt to trick the user into unintentionally clicking an unexpected web page element. In another word, the attacker hijacks the clicks of the victim that aren't meant for the exact page, but for a page where the hacker wants you to be.

PHISHING

Phishing is a hacking technique using which a hacker replicates the most-accessed sites and traps the victim by sending that spoofed link. Once the victim tries to login or enter some data, the hacker gets that private information of the target victim using the trojan running on the fake site.

VIRUS TROJAN

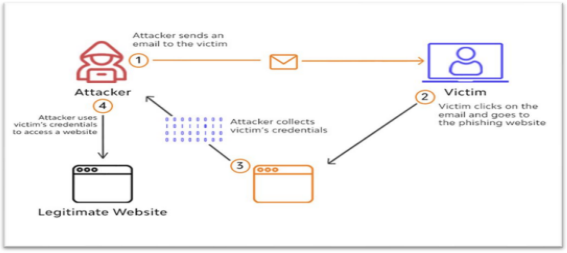
Virus or Trojans are malicious software programs which get installed into the victim's system and keeps sending the victims data to the hacker.

COOKIE THEFT

The cookies of a browser keep our personal data such as browsing history, username, and password for different sites that we access. Once the hacker gets the access to your cookie, he can even authenticate himself as you on a browser.

BAIT AND SWITCH

Using Bait and Switch hacking technique, the hacker runs a malicious program which the user believes to be authentic. This way, after installing the malicious program on your computer, the hacker gets unprivileged access to your computer.

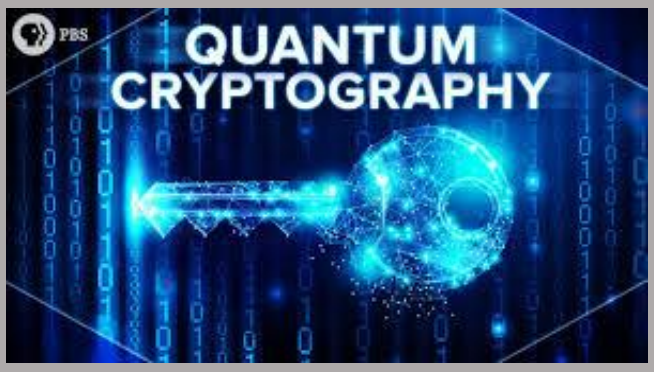


Conclusion

Computer Security is a continuous battle as computer security gets tighter hackers are getting smarter. In the preceding sections we saw the methodology of hacking, why should we aware of hacking and some tools which a hacker may use. Now we can see what can we do against hacking or to protect ourselves from hacking. The first thing we should do is to keep ourselves updated about those software's and we use only those software's from official and reliable sources.

Quantum Cryptography: Securing Information in the Quantum Realm

Mr. Debajit Sensarma
Department of Computer Science



Introduction

In the digital age, the escalating need for secure communication has necessitated the development of more sophisticated cryptographic methods. Traditional cryptography relies on mathematical complexities to safeguard information, but with advancements in computational power, particularly due to the emergence of quantum computing, these conventional methods are increasingly vulnerable. Quantum cryptography offers a revolutionary approach, utilizing principles of quantum mechanics to create secure communication channels theoretically unattainable through classical methods. This write-up explores the foundations, protocols, advantages, and challenges associated with quantum cryptography.

Understanding Quantum Mechanics

To appreciate quantum cryptography, one must first understand the principles of quantum mechanics. Quantum mechanics describes the behavior of particles at the subatomic level, where standard intuitions about physics no longer hold. Two fundamental principles relevant to quantum cryptography are superposition and entanglement.

1. **Superposition**: Unlike classical bits, which can exist in one of two states (0 or 1), quantum bits, or qubits, can exist in multiple states simultaneously. This superposition allows qubits to perform multiple calculations at once.
2. **Entanglement**: Quantum entanglement is a phenomenon where two or more particles become interconnected such that the state of one particle instantaneously influences the state of the other, regardless of distance. This property can be harnessed for secure information sharing.

The Need for Quantum Cryptography

The advent of quantum computing poses significant threats to traditional cryptographic algorithms, such as RSA and ECC (Elliptic Curve Cryptography). Quantum computers can efficiently solve problems deemed intractable for classical computers, including integer factorization and discrete logarithms, thereby jeopardizing the security of information encrypted using traditional methods. Consequently, a new paradigm is required—hence the

interest in quantum cryptography, which provides security based on the laws of physics rather than mathematical assumptions.

Quantum Key Distribution (QKD)

The most prominent application of quantum cryptography is Quantum Key Distribution (QKD). QKD allows two parties to create a shared, secret encryption key that can be used for secure communication. The security of QKD is grounded in the principles of quantum mechanics, making it resilient against eavesdropping attempts. If an eavesdropper, often referred to as "Eve," measures or intercepts the qubits being exchanged, the disturbance caused by such observation can be detected, enabling the legitimate parties, commonly referred to as "Alice" and "Bob," to take precautions.

BB84 Protocol

Developed by Charles Bennett and Gilles Brassard in 1984, the BB84 protocol was the first QKD scheme and remains one of the most widely studied. Here's a brief overview of how the BB84 protocol works:

1. **Preparation**: Alice prepares her qubits in one of four polarization states: horizontal (0), vertical (1), diagonal (±45 degrees).
2. **Transmission**: Alice sends these qubits to Bob over a quantum channel.
3. **Measurement**: Bob randomly selects a basis (either the standard basis or the diagonal basis) for each qubit and measures their polarization.
4. **Sifting Key**: After transmission, Alice and Bob publicly share their basis choices. They retain only the bits where they both used the same basis, generating a shared key.
5. **Error Rate Estimation**: Alice and Bob compare a subset of their results to estimate the error rate. If the error rate exceeds a predetermined threshold, they discard the key as it indicates eavesdropping.
6. **Final Key Generation**: If no significant interference is detected, Alice and Bob proceed to use the shared key for encryption.

Advantages of Quantum Cryptography

1. **Unconditional Security**: The security of quantum cryptography derives from the laws of quantum mechanics rather than computational assumptions. This characteristic allows for secure communication even against adversaries with unlimited computational power.
2. **Eavesdropping Detection**: Since any attempt to measure a quantum system inevitably alters its state, eavesdropping attempts can be detected. This feature enhances trust in the communication channel.
3. **Future-Proofing**: As quantum technology continues to advance, including the potential development of quantum computers, the fundamental security provided by quantum cryptography remains valid.

Challenges and Limitations

Despite its advantages, quantum cryptography faces several challenges:

1. **Technological Limitations**: The implementation of quantum cryptography requires specialized hardware, including single-photon sources and detectors, which can be expensive and difficult to operate.
2. **Distance Limitations**: Quantum signals deteriorate over long distances due to absorption and scattering in optical fibers. While quantum repeaters and other technologies are being researched to mitigate this issue, they are still in development stages.
3. **Integration with Classical Systems**: The implementation of quantum cryptographic systems in existing classical communication infrastructures poses integration challenges. Bridging the gap between quantum and classical systems requires careful planning and innovation.
4. **Key Distribution Rates**: The rate of key generation through QKD can be significantly lower than that of traditional methods, which may limit its practical applications in high-speed networks.

Future Prospects

The potential applications of quantum cryptography extend beyond secure communication. Future prospects include:

1. **Secure Multi-Party Computation**: Quantum cryptography could facilitate secure computations among multiple parties without revealing their inputs, enhancing privacy in collaborative environments.
2. **Post-Quantum Cryptography**: As quantum computers evolve, hybrid systems leveraging both quantum and classical cryptographic methods could ensure broader security against future threats.
3. **Quantum Networks**: Researchers are exploring the concept of quantum internet, which would enable the sharing of qubits among multiple users, facilitating advanced cryptographic protocols and secure communication on a larger scale.

Conclusion

Quantum cryptography represents a groundbreaking step in the field of secure communication, marrying the principles of quantum mechanics with cryptographic techniques to create theoretically unbreakable channels. While challenges remain in its implementation and practical application, the rapid advancement of this technology promises a future where secure communication can thrive in an increasingly complex digital landscape. As research continues and technologies mature, quantum cryptography is poised to play a pivotal role in safeguarding information in the quantum era.

Applications of Artificial Intelligence in Security

Mr. Ashadul Haque
Department of Computer Science

Introduction

As the digital landscape expands, the importance of cybersecurity has escalated dramatically. High-profile data breaches, identity theft, and cyberattacks present significant threats to individuals, businesses, and governments. In this context, Artificial Intelligence (AI) has emerged as a transformative technology, revolutionizing how security measures are developed and implemented. AI enhances the effectiveness and efficiency of security practices across various sectors, from cyberspace to physical security. This write-up delves into the applications of AI in security, exploring its impact on threat detection, incident response, fraud prevention, and more.

1. AI in Cybersecurity

AI has profoundly impacted the field of cybersecurity, significantly improving threat detection and response capabilities. The ability to analyze vast amounts of data and identify patterns makes AI a valuable asset in combating cyber threats.

a. Threat Detection

Traditional cybersecurity systems often rely on predefined rules and signatures to identify threats. However, cybercriminals continually evolve their tactics, making it challenging for legacy systems to keep pace. AI-driven systems utilize machine learning algorithms to analyze network traffic and user behavior, enabling them to detect anomalies that may indicate a security breach.

For example, AI can identify unusual patterns in login attempts, such as multiple failed logins from different locations in a short time frame, suggesting a possible

account takeover. Through continuous learning from previous security incidents, AI systems incrementally improve their threat detection capabilities. Solutions like Darktrace and Vectra AI exemplify how machine learning can provide real-time threat detection and response.

b. Incident Response

When a security incident occurs, rapid and effective response is crucial to mitigate damage. AI plays a vital role in automating incident response processes. AI-driven systems can analyze security alerts, prioritize incidents based on severity, and even initiate predefined responses without human intervention.

For instance, platforms like IBM's Watson for Cyber Security leverage AI to assess incoming threats, correlate data from multiple sources, and recommend actions for security teams. By automating routine responses and providing actionable insights, AI enhances the speed and efficiency of incident response while allowing human analysts to focus on more complex tasks.

2. AI in Physical Security

AI is not limited to digital security; it also plays a pivotal role in enhancing physical security through advanced surveillance and threat assessment systems.

a. Video Surveillance and Analysis

AI-powered video analytics enable organizations to monitor environments more effectively. Video surveillance systems equipped with AI can analyze footage in real-time to identify suspicious behavior, track individuals, or detect unauthorized access.

Facial recognition technology is among the most notable applications of AI in physical security. Systems can match live footage against databases of known individuals, helping law enforcement and security personnel identify potential threats. However, this application raises ethical concerns regarding privacy and consent that must be addressed.

b. Smart Security Systems

AI also contributes to the development of smart security systems that integrate various technologies to enhance safety. For instance, smart access control systems can utilize biometric authentication—such as fingerprint or retina scanning—combined with AI algorithms to assess the risk associated with granting access based on user behavior and environmental conditions.

An example of such a system is the integration of AI-driven analytics in smart home security systems, where the technology learns the typical behavior patterns of residents and identifies anomalies, such as unexpected movements during unusual hours.

3. AI in Fraud Prevention

The financial sector is a significant beneficiary of AI, particularly in fraud detection and prevention. As digital transactions increase, so does the potential for fraudulent activities.

a. Transaction Monitoring

Machine learning models can analyze transaction patterns in real time, identifying anomalies that may indicate fraudulent behavior. For instance, if a credit card is used for a high-value purchase in a foreign country shortly after a domestic transaction, the system can flag this as suspicious. By employing AI, financial institutions can reduce false positives while improving the accuracy of fraud detection.

b. Identity Verification

AI enhances identity verification processes through advanced biometric technologies. Methods such as facial recognition, voice recognition, and behavioral analytics help ensure that users are who they claim to be, thereby reducing instances of identity theft and fraud. Companies like Jumio and IDology utilize AI-driven identity verification solutions that offer a seamless user experience while maintaining robust security standards.

4. AI in National Security

AI applications extend to national security, where they enhance intelligence analysis, threat assessment, and decision-making processes.

a. Predictive Analytics

AI can analyze vast datasets to identify potential security threats before they materialize. By assessing patterns and indicators from multiple sources, including social media, news articles, and surveillance data, AI can provide actionable intelligence to national security agencies. This capability supports proactive measures and preparedness against potential threats.

b. Autonomous Surveillance and Reconnaissance

Unmanned aerial vehicles (UAVs) and drones equipped with AI technologies are revolutionizing surveillance and reconnaissance. These autonomous units can conduct intelligence-gathering missions, assess threats, and provide real-time data without endangering human lives. AI algorithms enable these drones to navigate complex environments, recognize targets, and analyze gathered information swiftly.

5. Ethical Considerations and Challenges

Despite the numerous benefits of AI in security, challenges and ethical concerns accompany its deployment.

a. Privacy Concerns

The use of AI technologies, particularly in surveillance and data collection, raises significant privacy issues. Individuals may feel uncomfortable knowing their behavior is being monitored and analyzed. Striking a balance between security and privacy rights is crucial for ethical implementation.

b. Bias and Discrimination

AI systems can inadvertently perpetuate biases present in their training data, leading to discrimination against certain societal groups. For instance, flawed facial recognition systems have shown higher error rates for individuals with darker skin tones. Developers must take cautionary steps to ensure fairness and mitigate bias in AI algorithms.

c. Dependence on Technology

As reliance on AI for security increases, there is a risk of over-dependence on automated systems. Human oversight remains essential, particularly in decision-making processes that could have significant consequences. Combining AI capabilities with human expertise ensures checks and balances within security operations.

Conclusion

AI has become an integral part of modern security strategies, offering innovative solutions to the ever-evolving threats faced by individuals, organizations, and nations. Its applications in cybersecurity, physical security, fraud prevention, and national defense demonstrate its versatility and effectiveness. However, as the adoption of AI in security continues to grow, stakeholders must address the associated ethical concerns and challenges, ensuring that technological advancements serve to enhance security while protecting individual rights. The future of security will undoubtedly rely on the continued evolution and responsible implementation of AI technologies.

PHISHING (A Game of Deception)

Mr. Milan Das
Department of Computer Science

Phishing attack plays a dominant role in the digital threat landscape. It is a fraudulent method of trying to gather personal information using deceptive emails, SMS and websites. "Phish" is pronounced just like the word "fish"- the analogy is that an angler throwing a baited hook out there (the phishing email) and hoping you bite.
A phishing attack usually happens when an attacker dupes a victim to open an email or text message and to click a link or download an attachment. When this malicious link is clicked, malware is installed automatically and the freezing of the system can happen which leads to a ransomware attack or the revealing of sensitive information.
Phishing scams try to 1) infect device with malware, 2) Steal private credentials and personal information such as Card number, Password, PINs etc to get money or identity, 3) obtain control of online accounts etc.
Such attacks are increasingly popular because they are easy to conduct. A phishing attack can have devastating results for both individuals and for the company. It can cause severe financial losses in addition to declining market share, reputation, and consumer trust.

Here are some Costly Phishing Attacks:

$100 million — Facebook and Google
$75 million — Crelan Bank
$61 million — FACC
$50 million — Upsher-Smith Laboratories
$47 million — Ubiquiti Networks
$44 million — Leoni AG
$31 million — Xoom Corporation
$17 million — The Scoular Company
$11.8 million — MacEwan University
$3 million — Mattel

Now we shall look at some commonly used phishing attacks:

Email phishing: – Most of the phishing attacks are sent via email. Attackers will register fake domains impersonating real organizations and will send thousands of generic requests. Links usually lead to malicious websites that steal credentials or install malicious code, known as malware, on users' devices. Sometimes they use the organization's name in the local part of the

email address (such as amazon@domainregistrar.com) in the hope that the sender's name will only appear as "Amazon" in the recipient's inbox.

❖ **Whaling: –** Attackers use social media or company websites to find the names of the organization's CEO or other members of senior management. Then they impersonate the employees of that organization using a similar email address. Emails may require a money transfer or require the recipient to review documents. A whaling attack is also known as CEO fraud. Scams involving fake tax returns are an increasingly common type of whaling.
❖ **Vishing: –** Vishing is short for "voice phishing" which includes tricking people on the phone, persuading them to divulge sensitive information. In this type of attack, the attacker tries to steal the victim's data and use it.
For example, many people receive fake phone calls from people for Internal Revenue Service (IRS) during tax season saying that they want to do an audit and need a Social Security number. The recipient can be easily tricked into providing personal information in vishing attacks.

❖ **Smishing: –** Smishing is one type of Phishing attack that involves the use of text messages which are sent using SMS to trick people into giving up money or personal information. Often the text message includes a link that, when clicked, installs malware on the user's device.

❖ **Spear phishing –** This type of phishing attack uses email but with a specific targeted approach. The attackers use open-source intelligence (OSINT) to gather information about a particular company through social media or the company's website. Then, they make specific individuals from the company as their target using real names, job roles to make the recipient think the email has arrived from a known, legitimate source.

❖ **Pharming –** In a pharming attack, the attackers hack a Domain Name server (DNS). The domain names are translated into IP addresses with the help of DNS. Whenever a user types a URL in a browser, the server will redirect the user to a fraud or cloned website that may look exactly the same as an original or legitimate website.

Some recent Phishing Scams:

Coronavirus Phishing Scam: Coronavirus/COVID-19 phishing scams are the latest scams happening all around us. These emails and messages may look official but if we investigate the link or email id carefully, we will understand because government organizations never ask us personal information or bank details for COVID-19 Vaccination.
So, if we receive these types of emails, we should check for "HTTPS" and not 'HTTP" before clicking on these types of links because HTTPS is far more secure than HTTP.
But if we give our personal information, then without panic, we should reset our credentials on sites and contact our bank immediately to change the required credentials.

PhonePe Phishing scam: Few days before, I got a phone call from a scamster to complete few steps to receive the cashback on the PhonePe app by accepting a payment link which appeared on my notifications. But I did not do it.
Nowadays many people have also received an SMS message with a link claiming to be from various mobile payment apps and urging them to click and unlock exciting cashback rewards.
In this case if we click on the link and follow the steps to claim the reward, we will lose money to the fraudsters. So, in this type of cases, any message asking us to enter our UPI PIN to receive cashback should be ignored.

Here are some tips that we can use to defend us from phishing attack:

- We should always check the spelling of the URLs in email links before we click or enter sensitive information.

- The emails (requesting personal information, login-ID, and passwords or money transactions) should be double checked as this can lead to huge financial loss.
- We should be careful with notifications as they can include links that direct recipients to malicious websites.
- We should be aware of small mistakes like misspellings, strange fonts, mismatched content etc that can be found on malicious websites.
- We should not use the insecure or open Wi-Fi connections because an attacker may steal one's credentials when we will use the insecure network.
- We should not post our personal data, like our birthday, vacation plans, or our address or phone number publicly on social media.
- A firewall should be used to prevent traffic from malicious source because unwanted sources can download malware and other harmful content on our system.

However, Phishing is constantly evolving to adopt new forms and techniques. So, using the guide above, we can protect us from some of the most common types of phishing attacks but it doesn't mean that we will be able to spot every phishing attack. With that in mind, it's imperative that we should increase our awareness level about phishing day by day on an ongoing basis.