Assignment 2(D4 –D6)

1) Prepare a Case Study on the shortage of cybersecurity professionals in India, its impact on organizations, and the measures needed to address this challenge (Discuss the specific implications for the Indian context)

A) In today's computerized world, new risks emerge every hour of every day. Connecting to the Internet opens up the possibility of a hacker targeting your organization. Cybercrime is becoming big business and cyber risk a focus of organizations and governments globally. Monetary and reputational risks are high if organizations don't have an appropriate cybersecurity plan.

According to the 2023 India Threat Landscape Report by Singapore-based cybersecurity firm Cyfirma, India is the most targeted country globally, facing 13.7% of all cyber-attacks, the Economic Times reported. The US is the second most targeted country, with 9.6% of all attacks.

According to the report, India's cybersecurity workforce stood at around 0.3 million in 2023, up from 0.21 million in 2022, and 0.1 million in 2021.

India has been positioned as the 7th most breached country in the world during the second quarter of 2023

The survey also found that frustration stemmed from the skills shortage and the many changes in cybersecurity. Many of the leaders (52%) reported struggling with new frameworks and models, such as zero trust. One in five leaders also found the skill level of their team to be a serious challenge

There is currently a high demand for skilled cyber professionals in the job market. It is expected that by 2025 there will be 3.5 million unfilled cyber security jobs due to a lack of skilled professionals and a growing need to secure more and more systems.

In fact, AI and Machine Learning Specialists top the list of fast-growing jobs. Cybersecurity: The growing digitization of businesses and the increasing threat of cyber-attacks, will have cybersecurity professionals play a vital role in safeguarding digital assets.

Research shows the gap between global demand and cyber workforce capacity in 2022 was estimated at 3.4 million people, a 26% increase over the previous year. Meanwhile, Gartner predicts that by 2025, more than half of significant cyber incidents will come from a lack of talent as well as general human error and also a lack of skilled professionals which makes it challenging.

As the world is advancing in the realm of digitalisation, the threat of cyber-attacks has also grown and India is no exception to it. In October, 2023, Re security, a US company, informed the world about the availability of Indians' personal data on the dark web

- **Critical Infrastructure Vulnerability:** India's critical infrastructure, such as power grids, transportation systems, and communication networks, is vulnerable to cyber-attacks that can **disrupt essential services** and endanger public safety and national security.
  - For example, in October 2019, there was an attempted cyber-attack on the **Kudankulam Nuclear power plant.**
- **Financial Sector Threats:** The financial sector in India faces a high risk of cyber attacks from cybercriminals who seek to profit from stealing or extorting money. Attacks on banks, financial institutions, and online payment systems can cause financial losses, identity theft, and a loss of trust in the financial system.
  - For instance, in March 2020, a malware attack on the City Union Bank's **SWIFT system** led to unauthorised transactions worth USD 2 million.
- **Data Breaches and Privacy Concerns:** As India moves towards a digital economy, the amount of personal and government data stored online increases. This also increases the risk of data breaches, where hackers access and leak sensitive

information. Data breaches can have serious consequences for the privacy and security of individuals and organisations.

  - For example, in May 2021, the personally identifiable information (PII) and test results of 190,000 candidates for the 2020 Common Admission Test (CAT), used to select applicants to the IIMs, were leaked and put up for sale on a cybercrime forum.

- **Cyber Espionage:** Cyber espionage is the use of cyber attacks to spy on or sabotage the interests of other countries or entities. India, like other countries, is a target for cyber espionage activities that aim to steal confidential information and gain a strategic edge. Cyber espionage can affect India's national security, foreign policy, and economic development.

  - For example, in 2020, a cyber-espionage campaign called Operation Side Copy (a Pakistani threat actor) was uncovered, which targeted Indian military and diplomatic personnel with malware and phishing emails.

- **Advanced Persistent Threats (APTs):** APTs are complex and prolonged cyber-attacks, usually carried out by well-resourced and skilled groups. These attacks are designed to infiltrate and remain hidden in the target's network for a long time, allowing them to steal or manipulate data, or cause damage.

  - APTs are difficult to detect and counter, as they use advanced techniques and tools to evade security measures.
  - For example, in February 2021, a cyber-security firm called RedEcho revealed that a China-linked APT group had targeted 10 entities in India's power sector, with malware that could potentially cause power outages.

- **Supply Chain Vulnerabilities:** Supply chain vulnerabilities refer to the weaknesses in the software or hardware components that are used by government and businesses for their operations. Cyber attackers can exploit these vulnerabilities to compromise the systems and services that depend on these components, and cause widespread damage.

  - For example, in December 2020, a global cyber attack on Solar Winds, a US-based software company that provides network management tools, affected several Indian organisations, including the **National Informatics Centre (NIC),** the Ministry of Electronics and Information Technology (MeitY), and Bharat Heavy Electricals Limited (BHEL).

The Initiatives Regarding Cyber Security

- **National Cyber Security Policy:** This policy aims to build a secure and resilient cyberspace for citizens, businesses, and the government. It outlines various objectives and strategies to protect cyberspace information and infrastructure, build capabilities to prevent and respond to cyber attacks, and minimise damages through coordinated efforts of institutional structures, people, processes, and technology.
- **Cyber Surakshit Bharat Initiative:** This initiative was launched to raise awareness about cybercrimes and create safety measures for Chief Information Security Officers (CISOs) and frontline IT staff across all government departments.
- **Indian Cyber Crime Coordination Centre (I4C):** This centre was established to provide a framework and eco-system for law enforcement agencies to deal with cybercrimes in a comprehensive and coordinated manner. It has seven components, namely:
    - National Cyber Crime Threat Analytics Unit
    - National Cyber Crime Reporting Portal
    - National Cyber Crime Training Centre
    - Cyber Crime Ecosystem Management Unit
    - National Cyber Crime Research and Innovation Centre National Cyber Crime Forensic Laboratory Ecosystem
    - Platform for Joint Cyber Crime Investigation Team.
- **Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre):** This centre was launched in 2017 to create a secure cyberspace by detecting botnet infections in India and notifying, enabling cleaning and securing systems of end users to prevent further infections.
- **Computer Emergency Response Team - India (CERT-In):** It is an organisation of the **MeitY** which collects, analyses

and disseminates information on cyber incidents, and also issues alerts on cybersecurity incidents.

- **Critical information infrastructure (CII):** It is defined as a computer resource, the destruction of which, shall have debilitating impact on national security, economy, public health or safety.
  - The government has established the **National Critical Information Infrastructure Protection Centre (NCIIP)** to protect the CII of various sectors, such as power, banking, telecom, transport, government, and strategic enterprises.
- **Defence Cyber Agency (DCyA):** The **DCyA** is a tri-service command of the Indian Armed Forces that is responsible for handling cyber security threats. It has the capability to conduct cyber operations, such as hacking, surveillance, data recovery, encryption, and countermeasures, against various cyber threat actors.

What Should India Do Further to Save Itself from Cyber-attacks?

- **Strengthening Existing legal Framework:** India's primary legislation governing cybercrimes is the **Information Technology (IT) Act of 2000**, which has been amended several times to address new challenges and threats.
  - However, the IT Act still has some gaps and limitations, such as the lack of clear definitions, procedures, and penalties for various cyber offences, and the low conviction rate of cyber criminals.
  - India needs to **enact comprehensive and updated laws that cover all aspects of cyber security**, such as cyber terrorism, cyber warfare, cyber espionage, and cyber fraud.
- **Enhancing Cyber Security Capabilities:** India has several initiatives and policies to improve its cyber security, such as the National Cyber Security Policy, the Cyber Cells and Cybercrime Investigation Units, the Cyber Crime Reporting Platforms, and the Capacity Building and Training programs.

  - However, these efforts are still inadequate and fragmented, as India faces a shortage of technical staff, cyber forensics facilities, cyber security standards, and coordination among various stakeholders.
  - India needs to invest more in developing its human and technological resources, establishing cyber security centers of excellence, adopting best practices and standards, and fostering collaboration and information sharing among different agencies and sectors.
- **Establish a Cyber Security Board:** India must establish a cyber security board with government and private sector participants that has the authority to convene, following a significant cyber incident, to analyse what happened and make concrete recommendations for improving cybersecurity.
  - Adopt a zero-trust architecture, and mandate a standardised playbook for responding to cybersecurity vulnerabilities and incidents. Urgently execute a plan for defending and modernising state networks and updating its incident response policy.
- **Expanding International Cooperation:** India is not alone in facing the challenges of cyber security, as cyber-attacks transcend national boundaries and affect the global community.
  - India needs to engage more with other countries and international organisations, such as the **United Nations**, **the International Telecommunication Union**, **the Interpol**, and the Global Forum on Cyber Expertise, to exchange best practices, share threat intelligence, harmonise cyber laws and norms, and cooperate in cyber investigations and prosecutions.
  - India also needs to participate more actively in regional and bilateral dialogues and initiatives, such as the **ASEAN Regional Forum**, the **BRICS**, and bilateral forums it has like **Indo-US Cyber Security Forum,** to build trust and confidence, and to address common cyber security issues and interests**.**

2) Analyse a significant cyber-attack(s) that has affected an Indian organization institution. Evaluate the specific challenges faced, the response to the incident, and the lessons learned.

A) AIIMS Cyber Attack: A Grave Wake-up Call for India's Safety

In November 2022, the premier medical institute in the country, All India Institute of Medical Sciences New Delhi (AIIMS) was crippled by a major cyber-attack. Most of its servers stopped working as also the e Hospital network. All functions including the emergency, out-patient, in-patient and laboratory wings had to be shifted to manual management. This article discusses the issue of cyber attacks, especially on Critical Information Infrastructure in detail.

This case study focuses on the AIIMS attack, but other incidents like the 2019 Kolkata Airport attack or the 2023 Indian Army hack can be analysed similarly

The investigation into the AIIMS cyberattack revealed that the servers used in the cyberattack might have originated in China and Hong Kong

RANSOMWARE ATTACK ON AIIMS

DEVELOPMENTS SO FAR

On 23 November 2022, patients and doctors complained about the hospital's services working slowly or not at all. As a result, the hospital was forced into working in a manual mode.

- The National Informatics Centre investigated the issue and found signs of a ransomware attack on the hospital's servers.

- The attack corrupted all the files stored on the main and backup servers of the hospital.
- The cyber-attack derailed many day-to-day activities at AIIMS, with OPD registrations and blood sample reports being halted at the premier institute. While AIIMS was able to restart some of these services, records were being kept manually causing delays and inconvenience to medical personnel and patients alike.
- The breach in security has particularly affected the e-hospital application, which was provided and managed by NIC since 2011-12, stopping the online functioning of OPD, emergency, and other patient care services on the AIIMS premises.
- On 30 November 2022, AIIMS decided to get four new servers from the Defence Research and Development Organisation (DRDO) so it can resume its e-hospital facility for patients.
- On 16 December 2022, Replying to another question in the LokSabha, Minister of State for Health and Family Welfare said

  All the data for e-Hospital had been retrieved from a backup server and restored on new servers.

  Most of the functions of e-Hospital application such as patient registration, appointment, admission, discharge etc. had been restored after two weeks of the attack.

- Probe agencies have still not located the person, organisation and exact physical location linked to the cyber-attack. However, they have tracked a server address in China, which could be an indication towards state sponsored cyber warfare which was already flagged by various cyber threat intelligence firms.

IMPACTS AND RAMIFICATIONS

- The organisation’s critical data is encrypted so that they cannot access files, databases, or applications stored on the main and backup servers of the hospital.
- The cyber-attack has frozen everyday work at AIIMS, including appointments and registration, billing, laboratory report generation, etc.
- The exploited databases also contained personally identifiable information of patients and healthcare workers — and administrative records on blood donors, ambulances, vaccination and caregivers, and employee log-in credentials.
- The data breach has reportedly compromised the data of nearly 3–4 crore patients, including sensitive data and medical records of several

VIPs including former prime ministers, ministers, bureaucrats, and judges,

RESPONSE OF SECURITY AGENCIES

Multi-agency investigation: The extent and threat of the attack was so much that multiple agencies like Delhi Police, the Centre's Computer Emergency Response Team (CERT-In), the Ministry of Home Affairs, and even the National Investigation Agency have joined the probe.

- A case of extortion and cyber terrorism was registered by the Intelligence Fusion and Strategic Operations (IFSO) unit of the Delhi Police since the attackers made an undisclosed (allegedly Rs. 200 Crore) demand to be sought in crypto currency in exchange for a key that would decrypt the data.
- The Delhi Police's use of the provisions of section 66 (F) of the Information Technology Amendment Act 2008 identifying this incident as a case of cyber terrorism is significant and indicates a much larger ambit than a typical ransomware case.
- The Computer Emergency Response Team (CERT-In) and National Informatics Centre worked on the hospital's servers to restore functionality.

FINDINGS

- CERT-In, the country's premier cybersecurity agency, has found that the hackers had two Proton mail addresses – "dog2398" and "mouse63209".
- They also found that 'dog2398' and 'mouse63209' were generated in the first week of November 2022 in Hong Kong. They also found that another encrypted file was sent from China's Henan.
- The targeted servers were infected with three ransomware: Wammacry, Mimi Katz and Trojan.
- The investigation also revealed that the main server and applications responsible for OPD services were down as all the system files in the home directory were encrypted by changing their extension to .bak9 – a new file that encrypted the extension files of the system.
- As per CERT-In's preliminary diagnosis, the cyberattack was the result of an "unorganised ICT (information and communications technology) network without centralised monitoring or system administration".
- This means the infected devices were connected to each other and the data on all of them could be accessed from every connected device — and no team was monitoring who was accessing these systems.

We learn from the AIIMS cyber-attack is the importance of regular data backups. It emphasized the importance of regular data backups to mitigate the impact of ransomware attacks

The analysis can be expanded to include the long-term impact and ongoing challenges faced by AIIMS and the Indian healthcare sector post-attack

The most recent cyberattack in India was against the e-Nagarpalika portal of Madhya Pradesh, where the data of people living in 413 cities was compromised. The cyberattack brought to light how smaller government portals have low security but highly sensitive data. Recently, US real estate giant First American also got hit by a massive cyberattack, with the organisation forced to take some of its operations offline due to compromised data.

Indian businesses are seeing technology disruptors as opportunities, with 69 per cent of Indian executives seeing Generative AI as an opportunity (against 60 per cent globally).

3) Investigate the top cybersecurity problems faced by universities and colleges, with a focus on the specific types of cyber-attacks targeting higher education institutions.

A) Higher education networks are especially vulnerable to attacks because of the highly collaborative nature of research and scholarship. Cyber attacks might not be completely avoidable, but there are steps that campus leaders can take to reduce the odds of a successful attack and protect sensitive information.

The education sector has emerged as the most targeted industry for cyber-attacks, accounting for more than 7 lakh detected threats in April-June 2023, according to a study. The substantial number of attacks underscores the increasing vulnerability of educational institutions to cyber-attacks, the study said.

Social engineering is the most significant threat to the education sector. This includes mostly phishing attacks and ransomware attacks.

Institutions of higher learning face a constant deluge of cyber-attacks. Following an incident in 2015, Kevin Morooney – former Vice Provost for Information Technology at Pennsylvania State University – told The New York Times that Penn State faced an average of 20 million attacks per day, an amount "typical for a research university."

Cybersecurity is a massive concern for colleges and universities,

Particularly in a post-pandemic world. Even before the pandemic hit, institutions of higher education already collected massive amounts of data from students and faculty. This has been heightened now that many universities are offering hybrid or fully remote curriculums.

Because colleges and universities store such massive amounts of data, they are often a target of hackers and other cyber criminals. **Cyber-attack statistics** reflect this. In fact, there were **1,851 data breaches** in educational institutions between 2005 and 2021. Additionally, many universities have outdated or poorly constructed cybersecurity systems, which makes them even more vulnerable.

With so many cybersecurity threats looming, institutions of higher learning will need to take steps to prevent them. Understanding the types of security threats that are most relevant to colleges and universities can help you develop an effective cybersecurity strategy. In this article, we'll take a look at the top   cybersecurity threats facing universities today and how to address them.

1. Phishing

Phishing is a very common problem for colleges and universities. In a phishing attack, the hacker will pose as a trusted entity and exploit that trust to trick the user into providing sensitive information like passwords or even social security numbers. Phishing typically happens through email or social media messaging.

There are a few ways that hackers typically choose to target colleges and universities via phishing. The first is by posing as the college in order to gain access to student or faculty login information. The hacker can then use this information to access the university's digital systems and uncover many different types of valuable data.

Another strategy is to target university presidents or specific faculty members. These people may have access to specific pieces of data that hackers want, or they may simply be high-net-worth individuals. The hacker will study the target individual's behaviour to find the most effective way to gain their trust. This strategy is often referred to as "spear phishing" or "whaling".

Phishing scams are one of the most effective types of cyber attacks because they can be very difficult to identify and block. **Educating your students** and staff on how to recognize phishing messages can be incredibly effective at preventing successful attacks. This is particularly important because many students and faculty use their own electronic devices on campus, which may not have adequate security protection.

Using two-factor authentication can also be very effective at preventing phishing attacks. With two-factor authentication, students and faculty will need to enter a code sent to their email or phone number in addition to their password in order to log in to the university's system. Apps like Google Authenticator make it relatively easy to implement this security measure.

2. Ransomware

Ransomware is another major challenge facing colleges and universities today. Ransomware is a type of malicious software that locates valuable data on a target system and holds it for a ransom sum. Colleges and universities hold a large amount of valuable student data, and they also conduct valuable high-level research, which is why so many hackers use ransomware to target them.

A ransomware attack can have devastating consequences for any university. Ransom sums for these attacks can be extremely high and are often financially devastating. Additionally, these attacks compromise valuable data and can even shut down your systems for an extended period of time, making it very difficult to conduct normal operations. On top of that, ransomware can negatively affect a university's reputation for years to come.

A successful ransomware attack can disrupt the educational process, delay administrative functions, and potentially lose vital academic data.

Additionally, institutions may face hefty financial burdens from the ransom itself and subsequent cybersecurity upgrades, not to mention potential reputational damage. Such incidents highlight the importance of robust **cybersecurity protocols in the age of digital and remote education**.

To prevent ransomware, universities should have a robust firewall in place throughout the entire system and keep it updated. Additionally, making regular backups of your most important data can lessen the impact of a ransomware attack if it does happen. Working with a trustworthy IT provider can help you stay on top of your cybersecurity maintenance and prevent ransomware attacks.

3. SQL Injections

Many hackers use SQL injections when attacking higher learning institutions. In an SQL injection, the hacker will enter a piece of malicious code into a query box on your website. The most common query boxes are login pages and contact forms, but there are many others. The malicious code enables the hacker to access protected data. They can even alter this data by adding new information or deleting it altogether.

Colleges and universities are often particularly vulnerable to SQL injections because of the number of query boxes on their website. There are ways to prevent SQL injections when designing your website by using parameterized statements. Working with an IT company through the web design process and updating your website to address these security threats can make a huge difference.

4. Data Breaches

There are many other types of data breaches that colleges and universities are vulnerable to. For example, there are many different types of malware that hackers have used over the years. As technology evolves, cybercriminals have gotten increasingly sophisticated and developed new strategies to gain access to valuable pieces of data. Human error can also increase the chances of a data breach.

5. Outdated Technology

Many universities use outdated technology, which puts them even more at risk for cyber-attacks. Missing even one software update can make your organization more vulnerable.

Educational technology is constantly evolving, and universities should regularly assess the devices and programs they are using to ensure they are still safe. Additionally, it's very important to schedule time for regular software updates. While upgrading to the latest technology can be pricey, think of it as an investment in the safety of your organization, your staff, and your students.

Cybersecurity risks are present for any institution of higher learning, regardless of the size of your organization or where you're located. If you don't already have some form of cybersecurity protection in place, now is the time to invest in this important service. This could mean hiring an in-house IT team for your university, or outsourcing to a managed services provider.

6. Malware

In an educational setting, malware can lead to data breaches, **compromising the personal information** of students, faculty, and staff. It can also disrupt online teaching platforms, potentially halting instruction or affecting grading and administrative systems.

In the era of remote education, where schools heavily rely on digital tools and online platforms, the spread of malware could lead to significant instructional delays, data loss, and privacy breaches. The recovery from a malware attack can be costly and time-consuming, potentially diverting resources from the core educational mission.

Therefore, robust cyber hygiene practices and a proactive approach to cybersecurity are crucial for today's educational institutions.

How to prepare and combat these threats in Education

As brave knights protect their kingdoms, we must prepare to defend our precious data and devices from these modern dangers.

This section will delve into essential strategies and practical tips to combat cyber security threats in educational institutions so we are equipped with the knowledge and tools to safeguard our valuable assets.

From guarding against hacker attacks to preventing data leaks, we'll navigate the path of security readiness step by step. By fostering a security-conscious culture and staying vigilant, we can create a safe and protected environment for all who seek knowledge within our walls.

So, gather your digital armour and join us to defend our educational realms. Let's face these challenges head-on and build a strong shield to thwart cyber assailants.

Incident response plan

An incident response plan outlines procedures to identify, respond to, and recover from cyber threats. It starts with preparation, which includes establishing a response team, identifying potential threats, and securing systems and data. Regular training sessions are conducted to ensure all educational community members, including students, teachers, and staff, are aware of best practices and understand their roles in cyber safety.

Two-factor or multi-factor authentication

Instead of relying solely on passwords, which can be cracked or stolen, **2FA/MFA** requires users to provide at least two forms of evidence to verify their identity.

This approach can be used to secure access to digital platforms, including learning management systems, email accounts, and administrative portals. Requiring this additional layer of authentication makes it significantly harder for attackers to gain unauthorized access, even if they have acquired a user's password. This can prevent a variety of cyber threats, such as data breaches, phishing, and unauthorized access to systems and sensitive information

Access control implementation

In an educational environment, access control implementation could mean limiting access to certain systems and data to only authorized individuals, such as staff, faculty, or specific students.

Access control can be role-based, where permissions are assigned based on a user's role within the institution. For instance, a teacher might access grades and student data within their classes, while an administrative staff member might have broader access to student records. Discretionary and mandatory access controls can further specify permissions based on the owner's discretion or predetermined policies.

Effective access control is crucial in securing sensitive data in remote education, where learning and administrative tasks are conducted on digital platforms. It ensures that only authenticated and authorized users can access specific resources, mitigating the risk of unauthorized access, data breaches, and other cyber-attacks.

Software updates

This applies to everything from the operating systems on school-owned devices, the learning management systems used to administer courses, the software used for virtual meetings, and even the individual applications used by students and teachers. Ensuring all these elements are up-to-date helps safeguard sensitive information such as student data, grades, and personal information from breaches.

The need for regular software updates becomes even more significant in education. Students and faculty are accessing educational resources from various devices and networks, each with its potential vulnerabilities. Encouraging regular updates and ensuring that institutional software is kept up-to-date can help prevent cyber-attacks, ensuring the continuity of education and the security of the educational environment.

A strong security policy

A strong security policy should address specific needs like student data privacy, intellectual property protection, and the use of educational technology tools. It should clearly outline the roles and responsibilities of students, educators, and administrators in maintaining cybersecurity.

In the remote education environment, a security policy may include guidelines on using personal devices for educational purposes, securing home networks, and protecting sensitive data when studying or teaching from home. Furthermore, it should establish procedures for reporting and responding to cyber threats in a remote learning environment.

Anti-malware software

Anti-malware software can be installed on school-owned devices and servers to protect student records, staff information, and academic data. It provides real-time protection, scanning incoming files, emails, and downloads for potential threats and preventing their execution.

Data backup

Backups can protect a range of critical data, from student records and grades to lesson plans and research data. Regular backups ensure that even if the original data is compromised or lost, a recent copy is available for restoration, minimizing disruption to educational processes.

In the new world of remote education, where much of the educational activity takes place on digital platforms, maintaining regular and secure backups is paramount. These backups can be performed on local storage devices or in the cloud, offering further resilience by physically separating the backup data from the original data.

Awareness and training (students, teachers, and staff)

Cybersecurity education aims to equip students, teachers, and staff with the knowledge and skills to recognize and avoid potential cyber threats, such as phishing attempts, malware, or unsecured networks.

This could involve training on identifying suspicious emails, understanding the importance of strong, unique passwords, and recognizing the signs of a potential system breach. Regular updates on new and evolving threats can help the school community stay vigilant and informed.

It's essential that cybersecurity awareness extends to the remote education methodology as well. Training can include best practices for securing home networks, using approved software and platforms, and ensuring data privacy while participating in online learning.

Hiring a security service provider

A security service provider could help set up robust firewalls, monitor network traffic for unusual activities, implement intrusion detection and prevention systems, and ensure regular software updates and data backups. They can also assist in developing strong security policies and incident response plans and conduct cybersecurity awareness training for students, teachers, and staff.

In the remote education scenario, where the digital footprint of educational institutions expands to include a variety of devices, networks, and platforms, a security service provider can help maintain a high level of cybersecurity. They can implement secure access controls for digital resources, secure cloud-based platforms used for remote learning, and provide guidance on securing home networks. They can also offer solutions for securely using personal devices for educational purposes, a common occurrence in remote education.

Prey can greatly assist in preventing and mitigating cyber attacks in the educational sector, especially within the context of remote education. It offers robust security solutions and anti-theft services that are crucial for managing and protecting a wide array of devices used in educational settings.

4) Select and analyse three real-world malware attacks, covering different malware types such as viruses, worms, and ransomware. For each case, describe the attack vector, the target, the impact.

A) Viruses and other malware spreading for sinister or baffling reasons has been a staple of cyberpunk novels and real-life news stories alike for decades. And in truth, there have been computer viruses on the internet since before it was the internet. This article will take a look at some of the most important milestones in the evolution of malware: These entries each represent a novel idea, a lucky break that revealed a gaping security hole, or an attack that turned to be particularly damaging—and sometimes all three.

1. Creeper virus (1971)
2. Brain virus (1986)
3. Morris worm (1988)
4. ILOVEYOU worm (2000)
5. Mydoom worm (2004)
6. Zeus Trojan (2007)
7. Crypto Locker ransomware (2013)
8. Emotet Trojan (2014)
9. Mirai botnet (2016)
10. Petyaransomware/NotPetya wiper (2016/7)
11. Clop ransomware (2019-Present)
12. Qbot(latest)

1. Creeper virus (1971)

Computer pioneer John von Neumann's posthumous work *Theory of Self-Reproducing Automata*, which posited the idea of computer code that could reproduce and spread itself, was published in 1966. Five years later, the first known computer virus, called Creeper, was a written by Bob Thomas. Written in PDP-10 assembly language, Creeper could reproduce itself and move from computer to computer across the nascent ARPANET.

Creeper did no harm to the systems it infected—Thomas developed it as a proof of concept, and its only effect was that it caused connected teletype machines to print a message that said **“I’M THE CREEPER: CATCH ME IF YOU CAN.”** We’re mentioning it here despite its benign nature because it was the first, and set the template for everything that followed. Shortly after Creeper’s release, Ray Tomlinson, best known for implementing the first email program, wrote a rival program called Reaper that spread from computer to computer eliminating Creeper’s code.

Creeper was designed to leap across computer networks, but for most of the 1970s and ’80s that infection vector was in limited simply because most computers operated in isolation. What malware did spread from computer to computer did so via floppy disks. The earliest example is **Elk Cloner**, which was created by a 15-year-old as a prank and infected Apple II computers. But probably the most important of this generation of viruses was one that came to be known as Brain, and started spreading worldwide in 1986.

2. Brain virus (1986)

Brain was developed by computer programmers (and brothers) Amjad and Basit Farooq Alvi, who lived in Pakistan and had a business selling medical software. Because their programs were often pirated, they created a virus that could infect the boot sector of pirated disks. It was mostly harmless but included contact information for them and an offer to **“disinfect”** the software. Whether they could actually “fix” the problem isn’t clear, but as they explained 25 years later, they soon started receiving phone calls from all over the world, and were shocked by how quickly and how far Brain had spread (and how mad the people who had illegally copied their software were at *them,* for some reason). Today Brain is widely regarded as the first IBM PC virus, so we’re including it on our list despite its benign nature, and the brothers still have the same address and phone number that they sent out 25 years ago.

3. Morris worm (1988)

1988 saw the advent of a piece of malware called Morris, which could claim a number of firsts. It was the first widespread computer worm, which meant it could reproduce itself without needing another program to piggyback on. It targeted multiple vulnerabilities to help it spread faster and further. While not designed to do harm, it was probably the first malware to do real substantive financial damage, more than earning its place on this list. It spread incredibly swiftly—within 24 hours of its release, it had infected 10 percent of all internet-connected computers and created multiple copies of itself on each machine, causing many of them to grind to a halt. Estimates of the costs of the attack ranged into the millions.

The worm is named after its creator Robert Morris, who was a Cornell grad student at the time and meant it as a proof-of-concept and demonstration of widespread security flaws. Morris didn’t anticipate that it would spread so quickly or that its ability to infect individual computers multiple times would cause so much trouble, and he tried to help undo the damage, but it was too late. He ended up the unfortunate subject of another first: The first person convicted under the 1986 Computer Fraud and Abuse Act.

3. ILOVEYOU worm (2000)

Unlike the previous malware creators on this list, Onel de Guzman, who was 24 in 2000 and living in the Philippines, crafted his creation with straightforward criminal intent: he couldn't afford dialup service, so he built a worm that would steal other people's passwords so he could piggyback off of their accounts. But the malware so cleverly took advantage of a number of flaws in Windows 95 especially the fact that Windows automatically hid the file extensions of email attachments so people didn't realize they were launching executable files that it spread like wildfire, and soon millions of infected computers were sending out copies of the worm and beaming passwords back to a Filipino email address. It also erased numerous files on target computers, causing millions of dollars in damage and briefly shutting down the U.K. Parliament's computer system.

De Guzman was never charged with a crime, because nothing he did was illegal in the Philippines at the time, but he expressed regret in an interview 20 years later, saying he never intended the malware to spread as far as it did. He also ended up being something of a pioneer in social engineering: the worm got its name because it spread with emails with "ILOVEYOU" in the subject line. "I figured out that many people want a boyfriend, they want each other, they want love, so I called it that," de Guzman said.

5. Mydoom worm (2004)

Mydoom may be almost 20 year old as of this writing, but as of today still holds a number of records. The Mydoom worm infected computers via email, then took control of the victim computer to email out more copies of itself, and did it so efficiently that at its height it accounted for a quarter of all emails sent worldwide, a feat that's never been surpassed. The infection ended up doing more than $35 billion in damages, which, adjusted for inflation, has also never been topped.

The creator and ultimate purpose of Mydoom remain mysteries today. In addition to mailing out copies of the worm, infected computers were also used as a botnet to launch DDoS attacks on the SCO Group (a company that aggressively tried to claim intellectual property rights over Linux) and Microsoft, which led many to suspect some rogue member of the open source community. But nothing specific has ever been proven.

6. Zeus Trojan (2007)

Zeus was first spotted in 2007, at the tail end of the Web 1.0 era, but it showed the way for the future of what malware could be. A Trojan that infects via phishing and drive-by downloads from infected websites, isn't just one kind of attacker; instead, it acts as a vehicle for all sorts of malicious payloads. Its source code and operating manual leaked in 2011, which helped both security researchers and criminals who wanted to exploit its capabilities. You'll usually hear Zeus referred to as a "banking Trojan," since that's where its variants focus much of their energy. A 2014 variant, for instance, manages to interpose itself between a user and their banking website, intercepting passwords, keystrokes, and more. But Zeus goes beyond banks, with another variation slurping up Salesforce.com info.

7. Crypto Locker ransomware (2013)

Zeus could also be used to create botnets of controlled computers held in reserve for some later sinister purpose. The controllers of one such botnet, called Gameover Zeus, infected their bots with Crypto Locker, one of the earliest prominent versions of what became known as ransomware. Ransomware encrypts many of the files on the victim's machine and demands a payment in crypto currency in order to restore access.

Crypto Locker became famous for its rapid spread and its powerful asymmetric encryption that was (at the time) uniquely difficult to break. It also became famous due to something unusual in the malware world: a happy ending. In 2014, the U.S. DoJ and peer agencies overseas managed to take control of the Gameover Zeus botnet, and restore the files of Crypto Locker victims free of charge. Unfortunately, Crypto Locker spread via good old-fashioned phishing as well, and variants are still around.

8. Emotet Trojan (2014)

Emotet is another piece of malware whose functionality has shifted and changed of the years that it has remained active. In fact, Emotet is a prime example of what's known as *polymorphic malware*, with its code changing slightly every time it's accessed, the better to avoid recognition by endpoint security programs. Emotet is a Trojan that, like others on this list, primarily spreads via phishing (repeat after us: *do not open unknown email attachments*).

Emotet first appeared in 2014, but like Zeus, is now a modular program most often used to deliver other forms of malware, with Trickster and Ryuk being two prominent examples. Emotet is so good at what it does that Arne Schoenbohm, head of the German Federal Office for Information Security, calls it the **"king of malware."**

9. Mirai botnet (2016)

All the viruses and other malware we've been discussing so far have afflicted what we think of as "computers" the PCs and laptops that we use for work and play. But in the 21st century, there are millions of devices with more computing power than anything that Creeper could have infected. These internet of things (IoT) devices are omnipresent, ignored, and often go unpatched for years.

The Mirai botnet was actually similar to some of the early malware we discussed because it exploited a previously unknown vulnerability and wreaked far more havoc than its creator intended. In this case, the malware found and took over IoT gadgets (mostly CCTV cameras) that hadn’t had their default passwords changed. Paras Jha, the college student who created the Mirai malware, intended to use the botnets he created for DoS attacks that would help settle scores in the obscure world of Minecraft server hosting, but instead he unleashed an attack that focused on a major DNS provider and cut off much of the U.S. east coast from the internet for the better part of a day.

10. Petya ransomware/NotPetya wiper (2016/7)

The ransomware Trojan dubbed Petra started afflicting computers in 2016. Though it had a clever mechanism for locking down its victims’ data it encrypts the master file table, which the OS uses to find files it spread via conventional phishing scams and wasn’t considered particularly virulent.

It would probably be forgotten today if not for what happened the following year. A new self-reproducing worm variant emerged that used the NSA’s leaked Eternal Blue and Eternal Romance exploits to spread from computer to computer. Originally distributed via a backdoor in a popular Ukrainian accounting software package, the new version—dubbed NotPetya—quickly wreaked havoc across Europe. The worst part? Though NotPetya still looked like ransomware, it was a wiper designed wholly to ruin computers, as the address displayed where users could send their ransom was randomly generated and did no good. Researchers believe that Russian intelligence repurposed the more ordinary Petya malware to use as a cyber weapon against Ukraine—and so, in addition to the massive damage it caused, NotPetya earns its place on this list by illustrating the symbiotic relationship between state sponsored and criminal hackers.

11. Clop ransomware (2019-Present)

Clop (sometimes written Cl0p) is another ransomware variant that emerged on the scene in 2019 and has grown increasingly prevalent since, to the extent that it was dubbed one of the top malware threats of 2022. In addition to preventing victims from accessing their data, Clop allows the attacker to exfiltrate that data as well. McAfee has a breakdown of the technical details, including a review of ways it can bypass security software.

What makes Clop so interesting and dangerous, however, is not how it's deployed, but by whom. It's at the forefront of a trend called Ransomware-as-a-Service, in which a professionalized group of hackers does all the work for whoever will pay them enough (or share in a percentage of the ransomware riches they extract from victims). The earlier entries in this list are from a day when the internet was for hobbyists and lone wolves; today, it seems even cybercrime is largely the province of governments and the professionals

12. QBOT

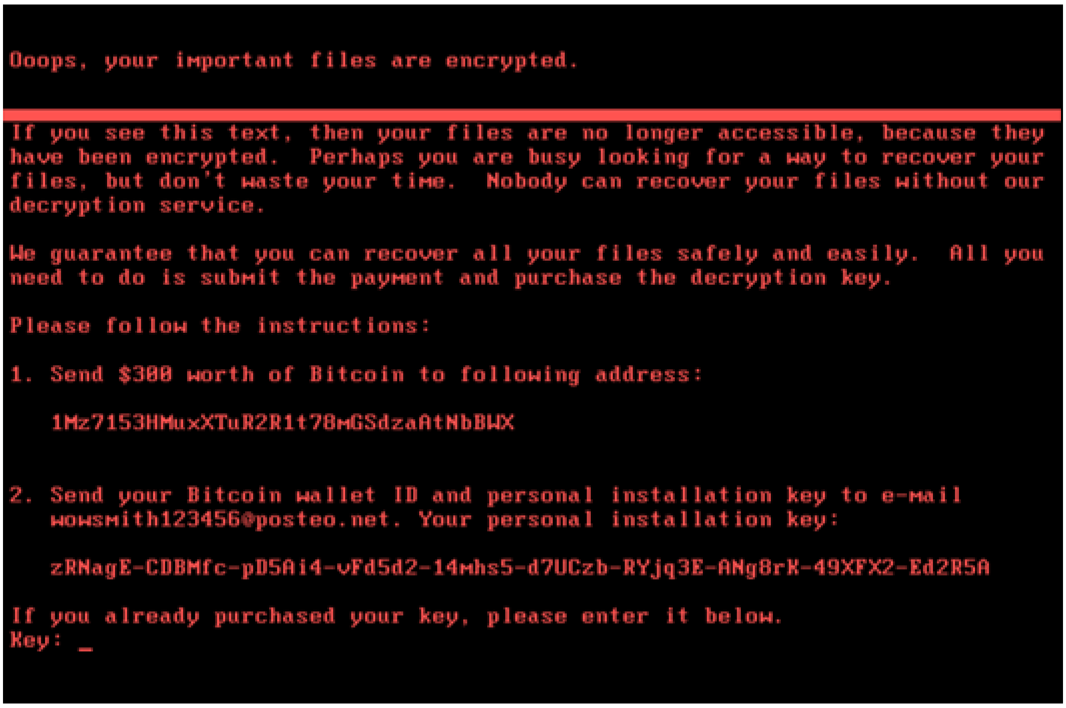
Qbot is mainly a banking Trojan and password stealer. It is worth noting that most variant are VM-aware and some have polymorphic abilities. Backdoor. Qbot main source are exploit kits but they are also spread by infected email attachments.

A leading provider of cybersecurity solutions globally, has published its Global Threat Index for June 2023. Researchers found that the Trojan Qbot has been the most prevalent malware so far in 2023, ranking first in five out of the six months to date.

There are many different variations of malware, you are most likely to encounter the following malware types: how they work and provide real-world examples of each.

1. Ransomware

Ransomware is software that uses encryption to disable a target's access to its data until a ransom is paid. The victim organization is rendered partially or totally unable to operate until it pays, but there is no guarantee that payment will result in the necessary decryption key or that the decryption key provided will function properly.



```
Ooops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they
have been encrypted.  Perhaps you are busy looking for a way to recover your
files, but don't waste your time.  Nobody can recover your files without our
decryption service.

We guarantee that you can recover all your files safely and easily.  All you
need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send $300 worth of Bitcoin to following address:

   1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX


2. Send your Bitcoin wallet ID and personal installation key to e-mail
   wowsmith123456@posteo.net. Your personal installation key:

   zRNagE-CDBMfc-pD5Ai4-vFd5d2-14mhs5-d7UCzb-RYjq3E-ANg8rK-49XFX2-Ed2R5A

If you already purchased your key, please enter it below.
Key: _
```

Example of a ransom letter

Ransomware Example:

This year, the city of Baltimore was hit by a type of ransomware named RobbinHood, which halted all city activities, including tax collection, property transfers, and government email for weeks. This attack has cost the city more than $18 million so far, and costs continue to accrue. The same type of malware was used against the city of Atlanta in 2018, resulting in costs of $17 million.

2. Fileless Malware

Fileless malware doesn’t install anything initially, instead, it makes changes to files that are native to the operating system, such as PowerShell or WMI. Because the operating system recognizes the edited files as legitimate, a fileless attack is not caught by antivirus software — and because these attacks are stealthy, they are up to ten times more successful than traditional malware attacks.

Fileless Malware Example:

Astaroth is a fileless malware campaign that spammed users with links to a LNK shortcut file. When users downloaded the file, a WMIC tool was launched, along with a number of other legitimate Windows tools. These tools downloaded additional code that was executed only in memory, leaving no evidence that could be detected by vulnerability scanners. Then the attacker downloaded and ran a Trojan that stole credentials and uploaded them to a remote server.

3. Spyware

Spyware collects information about users' activities without their knowledge or consent. This can include passwords, pins, payment information and unstructured messages.

The use of spyware is not limited to the desktop browser: it can also operate in a critical app or on a mobile phone.

Even if the data stolen is not critical, the effects of spyware often ripple throughout the organization as performance is degraded and productivity eroded.

Spyware Example:

DarkHotel, which targeted business and government leaders using hotel WIFI, used several types of malware in order to gain access to the systems belonging to specific powerful people. Once that access was gained, the attackers installed keyloggers to capture their targets passwords and other sensitive information.

4. Adware

Adware tracks a user's surfing activity to determine which ads to serve them. Although adware is similar to spyware, it does not install any software on a user's computer, nor does it capture keystrokes.

The danger in adware is the erosion of a user's privacy — the data captured by adware is collated with data captured, overtly or covertly, about the user's activity elsewhere on the internet and used to create a profile of that person which includes who their friends are, what they've purchased, where they've travelled, and more. That information can be shared or sold to advertisers without the user's consent.

Adware Example:

Adware called Fireball infected 250 million computers and devices in 2017, hijacking browsers to change default search engines and rack web activity. However, the malware had the potential to become more than a mere nuisance. Three-quarters of it was able to run code remotely and download malicious files.

EXPERT SUGGESTS THAT

Download Crowd Inspect: a free community tool for Microsoft Windows systems that is aimed to help alert you to the presence of potential malware are on your computer that may be communicating over the network.

5. Trojan

A Trojan disguises itself as desirable code or software. Once downloaded by unsuspecting users, the Trojan can take control of victims' systems for malicious purposes. Trojans may hide in games, apps, or even software patches, or they may be embedded in attachments included in phishing emails.

Trojan Example:

Emotet is a sophisticated banking Trojan that has been around since 2014. It is hard to fight Emotet because it evades signature-based detection, is persistent, and includes spreader modules that help it propagate. The Trojan is so widespread that it is the subject of a US Department of Homeland Security alert, which notes that Emotet has cost state, local, tribal and territorial governments up to $1 million per incident to remediate.

TrickBot malware is a type of banking Trojan released in 2016 that has since evolved into a modular, multi-phase malware capable of a wide variety of illicit operations.

6. Worms

Worms target vulnerabilities in operating systems to install themselves into networks. They may gain access in several ways: through backdoors built into software, through unintentional software vulnerabilities, or through flash drives. Once in place, worms can be used by malicious actors to launch DDoS attacks, steal sensitive data, or conduct ransomware attacks.

Worm Example:

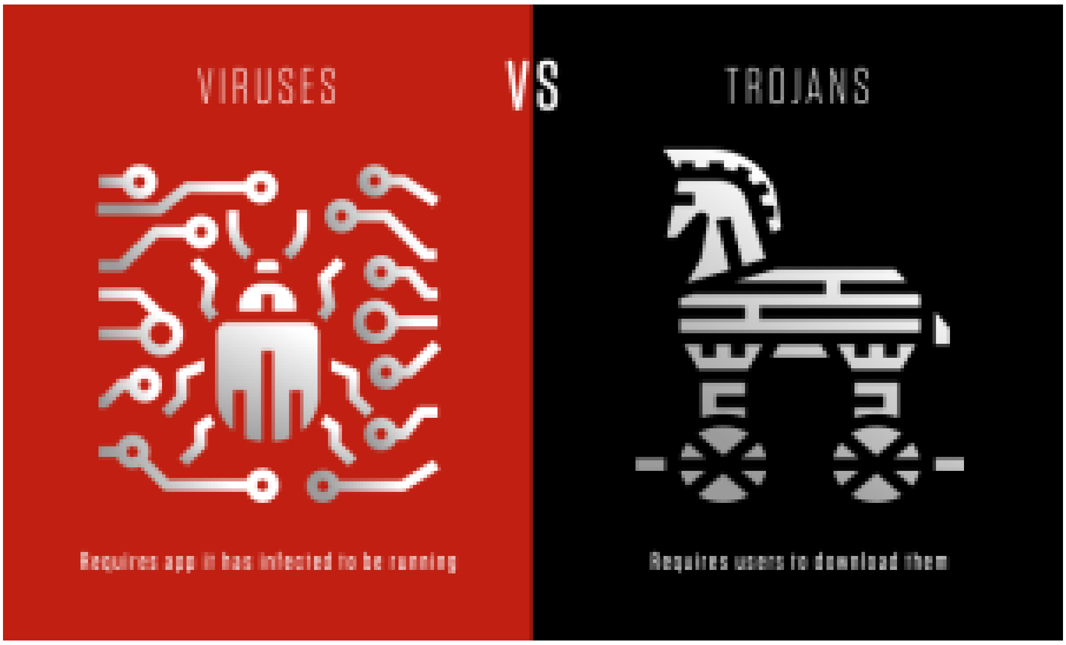
Stuxnet was probably developed by the US and Israeli intelligence forces with the intent of setting back Iran’s nuclear program. It was introduced into Iran’s environment through a flash drive. Because the environment was air-gapped, its creators never thought Stuxnet would escape its target’s network — but it did. Once in the wild, Stuxnet spread aggressively but did little damage, since its only function was to interfere with industrial controllers that managed the uranium enrichment process.

7. Virus

A virus is a piece of code that inserts itself into an application and executes when the app is run. Once inside a network, a virus may be used to steal sensitive data, launch DDoS attacks or conduct ransomware attacks.

Viruses vs. Trojans

A virus cannot execute or reproduce unless the app it has infected is running. This dependence on a host application makes viruses different from Trojans, which require users to download them, and worms, which do not use applications to execute. Many instances of malware fit into multiple categories: for instance, Stuxnet is a worm, a virus and a rootkit.


VIRUSES
VS
TROJANS
Requires app it has infected to be running
Requires users to download them

8. Rootkits

A rootkit is software that gives malicious actors remote control of a victim's computer with full administrative privileges. Rootkits can be injected into applications, kernels, hypervisors, or firmware. They spread through phishing, malicious attachments, malicious downloads, and compromised shared drives. Rootkits can also be used to conceal other malware, such as keyloggers.

Rootkit Example:

Zacinlo infects systems when users download a fake VPN app. Once installed, Zacinlo conducts a security sweep for competing malware and tries to remove it. Then it opens invisible browsers and interacts with content like a human would — by scrolling, highlighting and clicking. This activity is meant to fool behavioural analysis software. Zacinlo's payload occurs when the malware clicks on ads in the invisible browsers. This advertising click fraud provides malicious actors with a cut of the commission.

9. Keyloggers

A keylogger is a type of spyware that monitors user activity. Keyloggers have legitimate uses; businesses can use them to monitor employee activity and families may use them to keep track of children's online behaviours.

However, when installed for malicious purposes, keyloggers can be used to steal password data, banking information and other sensitive information. Keyloggers can be inserted into a system through phishing, social engineering or malicious downloads.

Keylogger Example:

A keylogger called Olympic Vision has been used to target US, Middle Eastern and Asian businessmen for business email compromise (BEC) attacks. Olympic Vision uses spear-phishing and social engineering techniques to infect its targets' systems in order to steal sensitive data and spy on business transactions. The keylogger is not sophisticated, but it's available on the black market for $25 so it's highly accessible to malicious actors.

10. Bots/Botnets

A bot is a software application that performs automated tasks on command. They're used for legitimate purposes, such as indexing search engines, but when used for malicious purposes, they take the form of self-propagating malware that can connect back to a central server.

Usually, bots are used in large numbers to create a botnet, which is a network of bots used to launch broad remotely-controlled floods of attacks, such as DDoS attacks. Botnets can become quite expansive. For example, the Mirai IoT botnet ranged from 800,000 to 2.5M computers.

Botnet Example:

Echobot is a variant of the well-known Mirai. Echobot attacks a wide range of IoT devices, exploiting over 50 different vulnerabilities, but it also includes exploits for Oracle Web Logic Server and VMWare's SD-Wan networking software. In addition, the malware looks for unpatched legacy systems. Echobot could be used by malicious actors to launch DDoS attacks, interrupt supply chains, steal sensitive supply chain information and conduct corporate sabotage.

11. Mobile Malware

Attacks targeting mobile devices have risen 50 percent since last year. Mobile malware threats are as various as those targeting desktops and include Trojans, ransomware, advertising click fraud and more. They are distributed through phishing and malicious downloads and are a particular problem for jailbroken phones, which tend to lack the default protections that were part of those devices' original operating systems.

Mobile Malware Example:

Triada is a rooting Trojan that was injected into the supply chain when millions of Android devices shipped with the malware pre-installed. Triada gains access to sensitive areas in the operating system and installs spam apps. The spam apps display ads, sometimes replacing legitimate ads. When a user clicks on one of the unauthorized ads, the revenue from that click goes to Triada's developers.

12. Wiper Malware

A wiper is a type of malware with a single purpose: to erase user data and ensure it can't be recovered. Wipers are used to take down computer networks in public or private companies across various sectors. Threat actors also use wipers to cover up traces left after an intrusion, weakening their victim's ability to respond.

Wiper Malware Example:

On Jan. 15, 2022, a set of malware dubbed *WhisperGate* was reported to have been deployed against Ukrainian targets. The incident is widely reported to contain three individual components deployed by the same adversary, including a malicious boot loader that corrupts detected local disks, a Discord-based downloader and a file wiper. The activity occurred at approximately the same time multiple websites belonging to the Ukrainian government were defaced.

An **attack** vector is a path or means by which an attacker or hacker can gain access to a computer or network server in order to deliver a **payload** or malicious outcome. Attack vectors enable hackers to exploit system vulnerabilities, including the human element.

Common cyber-attack vectors include viruses and **malware**, email attachments, webpages, pop-up windows, instant messages (IMs), chat rooms and deception. Except for deception, all of these methods involve programming or, in a few cases, hardware. Deception is when a human operator is fooled into removing or weakening system defences.

To some extent, firewalls and antivirus software can block attack vectors. But no protection method is totally attack-proof. A defines method can quickly become obsolete, as hackers are constantly updating attack vectors and seeking new ones in their quest to gain unauthorized access to computers and servers.

The most common malicious payloads are viruses, which can function as their own attack vectors, Trojan horses, worms and spyware. Third-party vendors and service providers can also be considered attack vectors, as they are a risk to an organization if they have access to its sensitive data.

How do cyber attackers exploit attack vectors?

Hackers have in-depth knowledge of the common security attack vectors that are available to them. When determining how to hack one of these security vectors, they first seek out vulnerabilities, or security *holes*, in these vectors that they think they can penetrate.

A security hole can be found in a piece of software or in a computer operating system (OS). Sometimes, a security vulnerability can open up because of a programming error in an application or a faulty security configuration. Hacks can even be low-tech, such as obtaining an employee's security credentials or breaking into a building.

Hackers are constantly scanning companies and individuals to identify all potential entry points into systems, applications and networks. In some cases, they may even target physical facilities or find vulnerable users and internal employees who will knowingly or inadvertently share their information technology (IT) access credentials.

What is the difference between attack vector and attack surface?

These two terms are often used interchangeably, but they are not the same thing. An attack vector differs from an **attack surface**, as the *vector* is the means by which an intruder gains access and the attack *surface* is what is being attacked.

One of the most publicized hacks was the Solar Winds supply chain attack. An investigation was undertaken to determine the attack vectors, but the breach may have been the result of compromised credentials or possible access through the development environment for Solar Winds' Orion IT management software.

10 of the most common attack vectors

Intruders are continuously seeking out new attack vectors. The most common attack vectors include the following:

1. **Software vulnerabilities.** If a network, OS, computer system or application has an unpatched security vulnerability, an attacker can use a threat vector, such as malware, to gain unauthorized access.
2. **Compromised user credentials.** Users can knowingly or inadvertently share their user IDs and passwords. This can be done verbally, but cyber attackers can also gain access to credentials through a brute-force attack that tries different combinations of user IDs and passwords until an authorized set of credentials is uncovered. The hacker then uses these credentials to hack a network, system or application.
3. **Weak passwords and credentials.** In brute-force attacks, cyber attackers focus their efforts on hacking user IDs and passwords that are weak or can be easily guessed. But hackers also steal credentials by using programs that monitor public Wi-Fi networks for when users input their access credentials. For example, a hacker could install keylogging software on a user's workstation

through an infected website or email. The keylogging program logs user keyboard activity, including the entry of the user's ID and password. Hackers can also gain access by enticing users to open unsolicited email attachments that contain malicious links to bogus websites that convince them to surrender personally identifiable information (PII).

4. **Malicious employees.** Malicious or disgruntled employees can hack into networks and systems using their security clearances to extract sensitive information, such as customer lists and intellectual property (IP) that they either demand ransom for or sell to others for nefarious purposes.
5. **Poor or missing encryption.** In some cases, employees -- or IT -- may forget to encrypt sensitive information stored on laptops and smartphones out in the field. In other cases, encryption techniques have known design flaws or only use limited keys to encrypt and protect data.
6. **Ransomware.** Ransomware is a type of malware that locks the data on the victim's computer, and the attacker either threatens to publish the victim's data or block access to it unless a ransom is paid. Ransomware can lock a user's files, often demanding a cash sum from the user in order to unlock the files. Most ransomware is inadvertently downloaded onto a computer or network by a user. It can come in the form of a file that a user opens that contains a worm, which is malware that spreads itself throughout a network, or a Trojan, which embeds malicious software code in a downloaded file that locks up the user's computer or data and then demands payment.
7. **Phishing.** Phishing is the deceptive practice of sending emails in which the attacker purports to be from a reputable company in order to lure individuals into revealing personal information, such as passwords or credit card numbers. Spear phishing is a highly targeted attack that targets a single recipient, seeking unauthorized access to sensitive company information.

8. **Misconfigured devices.** Companies can misconfigure their software and hardware security, which leaves them vulnerable to hackers. Vendor security pre-sets on equipment are lax, and if IT doesn't reconfigure this equipment before installing it on networks, security hacks can occur. In still other cases, companies purchase equipment and forget to fully configure security.

9. **Trust relationships.** In many cases, companies entrust their security to outside system and network vendors, cloud providers and business partners. When the systems of these third parties are breached, the information the hackers obtain may also contain sensitive information from the companies these providers service. Examples include when a major credit card carrier's network is breached or when a healthcare system is breached and sensitive data from patients is stolen.

10. **Distributed denial-of-service (DDoS) attacks.** DDoS attacks flood victims with bogus emails, rendering their system or network unusable and services unavailable to their intended recipients. These attacks often target the web servers of finance, commerce and government organizations and are often used to distract an organization from other network attacks.

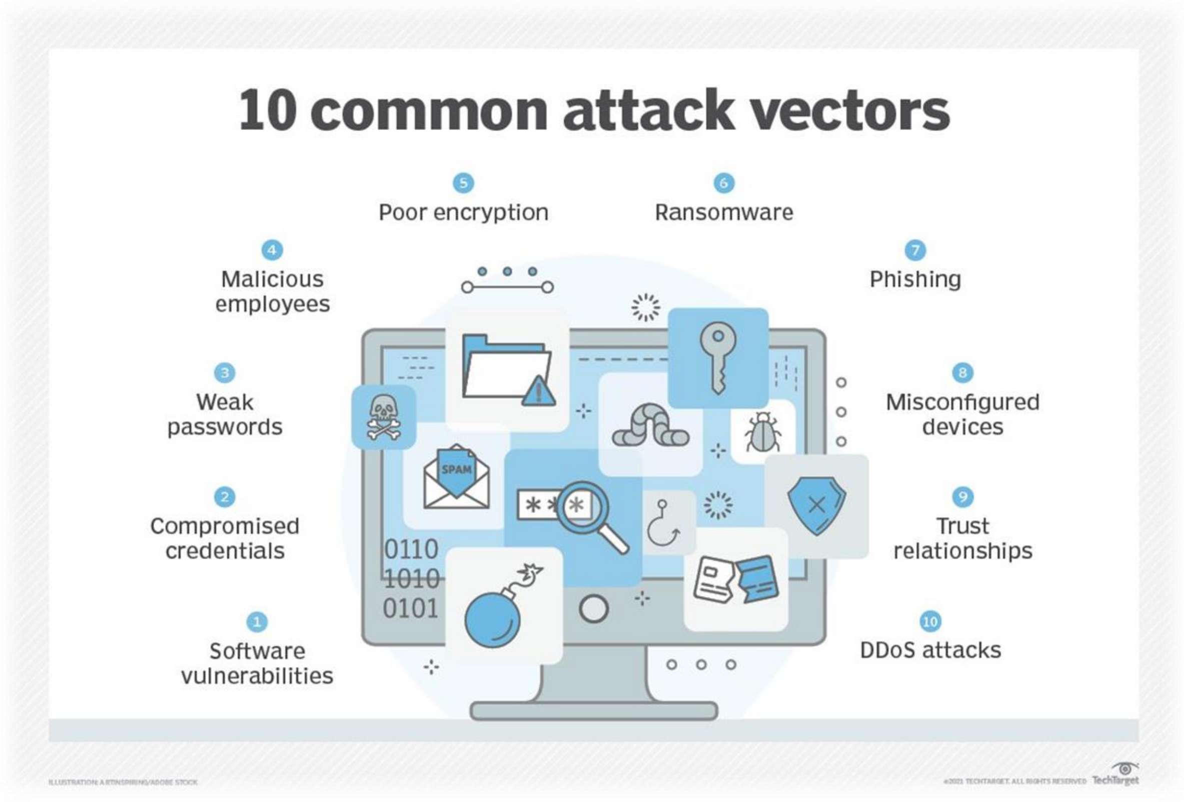


ILLUSTRATION: ARTINSPIRING/ADOBE STOCK

©2021 TECHTARGET. ALL RIGHTS RESERVED TechTarget

How to protect devices against common vector attacks

Attackers use a variety of techniques to penetrate corporate IT assets. As these techniques continue to evolve, IT's job is to identify and implement the policies, tools and techniques that are most effective in protecting against these attacks. The following is a list of effective protection techniques:

- **Implement effective password policies.** Ensure usernames and passwords meet proper length and strength criteria and the same credentials are not used to access multiple applications and systems. Use two-factor authentication (2FA) or verification methods, such as a password and a personal identification number (PIN), to provide an added layer of protection for system access.
- **Install security monitoring and reporting software.** This includes software that monitors, identifies, alerts and even locks down entry points to networks, systems, workstations and edge

technology once a potential attack by an unidentified or unauthorized user or source is detected.

- **Regularly audit and test IT resources for vulnerabilities.** At a minimum, IT vulnerability testing should be conducted quarterly, and an outside IT security audit firm should test IT resources for vulnerability annually. Based upon these findings, security policies, practices and prevention techniques should be updated immediately.
- **Keep IT security front and centre.** Security investments cost money, and a chief information officer (CIO) and a chief security officer (CSO) need the chief executive officer (CEO) and the board of directors to approve these purchases. This requires regular briefings and education for C-level executives so they understand the importance of securing IT and the ramifications for the company and its reputation if IT is left unsecured.
- **Train users.** All new employees should be provided comprehensive training in IT security policies and practices, and existing employees should be given refresher training annually. IT personnel, especially in the security area, should be current on the latest security policies and practices.
- **Collaborate with human resources (HR).** Social engineering vulnerability audits should be performed with an outside security audit firm at least once every two to three years. If there is suspicious employee activity, IT should immediately alert HR so it can take appropriate action, whether it is meeting with an employee, restricting an employee's access, coaching an employee or firing an employee.
- **Immediately install all updates.** Whenever a hardware, firmware or software update is issued, IT should promptly install it. If devices are used in the field, the security updates should be provided as push notifications, where software or firmware is automatically updated.

- **Use thin clients for companies with a bring your own device (BYOD) policy.** It is preferable to house all corporate data in a secure cloud or other enterprise system so users can sign in from home or from their own devices through a virtual private network (VPN), which is restricted to a specific set of users and is not open to the public. This eliminates sensitive data from being stored on remote devices.
- **Use strong data encryption** on portable devices. Whether a portable device is a laptop, a smartphone, a sensor or any other type of edge device, data encryption should be used wherever sensitive data is stored. This can be done by selecting a strong data encryption technology, such as Advanced Encryption Standard (AES). The U.S. government uses AES, which contains 192- and 256-bit keys for data encryption.
- **Review and set all security configurations** for OSes, internet browsers, security software, network hubs and edge devices, such as sensors, smartphones and routers. Often, systems, browsers, hubs and internet of things (IoT) devices come with minimal default security settings, and companies forget to adjust these settings. As a standard practice, companies should check and, if necessary, reset security on all new IT.
- **Secure physical spaces.** While most data breaches and security hacks target IT, physical access intrusions can also occur. Data centers, servers located in different business departments and remote field offices, medical equipment, field-based sensors and even physical file cabinets in offices are all hacking targets. They should be secured, protected and regularly inspected.

5) Provide Comparative Analysis on DES, AES, and RSA.

A) Information Security has become an important issue in data communication. Encryption has come up as a solution, and plays an important role in information security system. This security mechanism uses some algorithms to scramble data into unreadable text which can be only being decoded or decrypted by party those possesses the associated key. These algorithms consume a significant amount of computing resources such as CPU time, memory and battery power and computation time. This paper performs comparative analysis of three algorithm; DES, AES and RSA considering certain parameters such as computation time, memory usages and output byte. A cryptographic tool is used for conducting experiments. Experiments results are given to analyses the effectiveness of each algorithm

For secure communication over public network data can be protected by the method of encryption. Encryption converts that data by any encryption algorithm using the 'key' in scrambled form. Only user having access to the key can decrypt the encrypted data

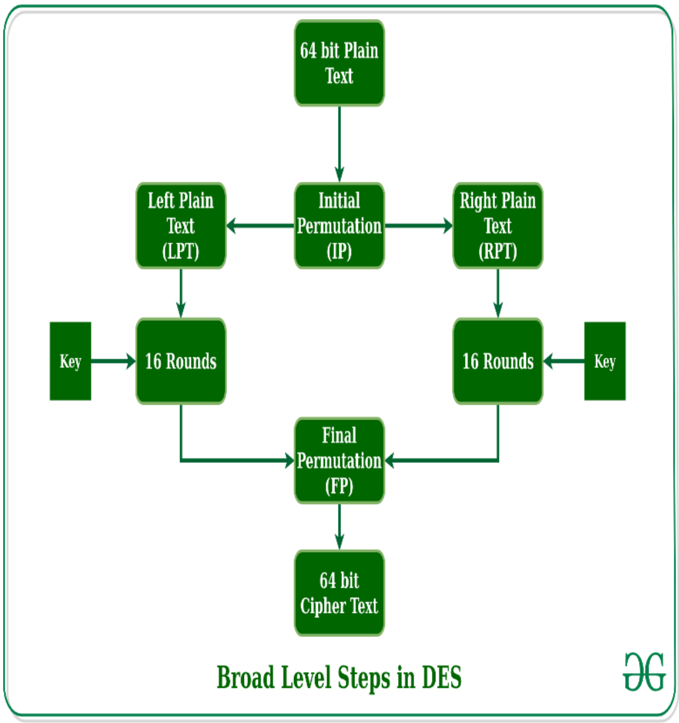
Encryption is a fundamental tool for the protection of sensitive information. The purpose to use encryption is privacy (preventing disclosure or confidentiality) in communications. Encryption is a way of talking to someone while other people are listening, but such the other people cannot understand what you are saying .

Encryption algorithms play a big role in providing data security against malicious attacks. In devices security is very important and different types of algorithms are used to prevent malicious attack on the transmitted data.

Encryption algorithm can be categorized into symmetric key (private) and asymmetric (public) key [1]. In Symmetric keys encryption or secret key encryption, only one key is used to encrypt and decrypt data. In Asymmetric keys, two keys are used; private and public keys. Public key is used for encryption and private key is used for decryption (e.g. RSA).

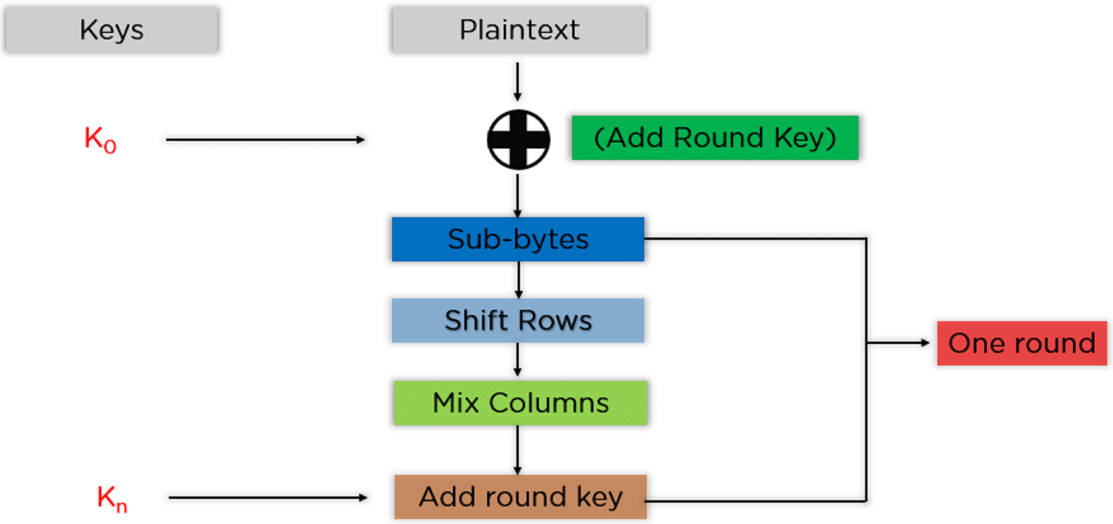
Data Encryption Standard (DES) Algorithm

DES Algorithms DES is a block cipher, with a 64-bit block size and a 56-bit key. DES consists of a16-round series of substitution and permutation. In each round, data and key bits are shifted, permutated, XORed, and sent through,8 s-boxes, a set of lookup tables that are essential to the DES algorithm. Decryption is essentially the same process, performed in reverse



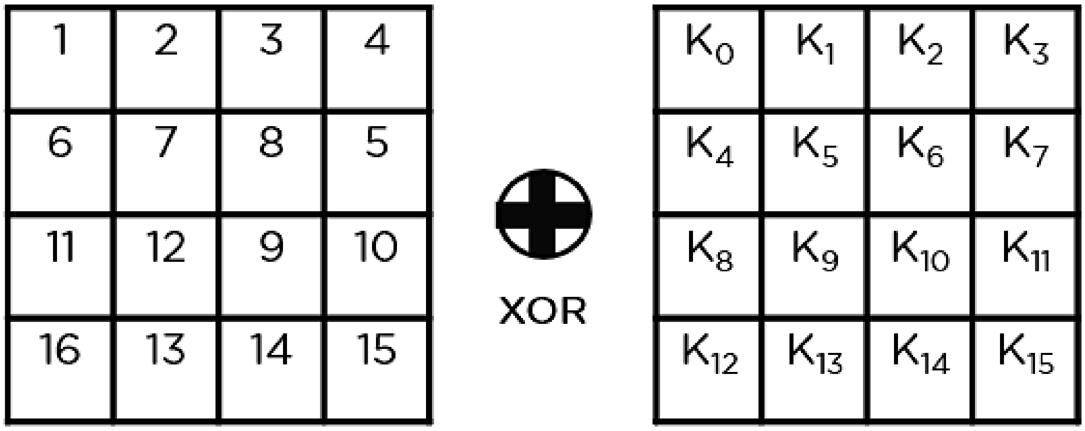
Advanced Encryption Standard (AES) Algorithm

AES Algorithm AES uses 10, 12, or 14 rounds. The key size that can be 128,192 or 256 bits depends on the number of rounds. AES uses several rounds in which each round is made of several stages. To provide security AES uses types of transformation. Substitution permutation, mixing and key adding each round of AES except the last uses the four transformations



The mentioned steps are to be followed for every block sequentially. Upon successfully encrypting the individual blocks, it joins them together to form the final ciphertext. The steps are as follows:

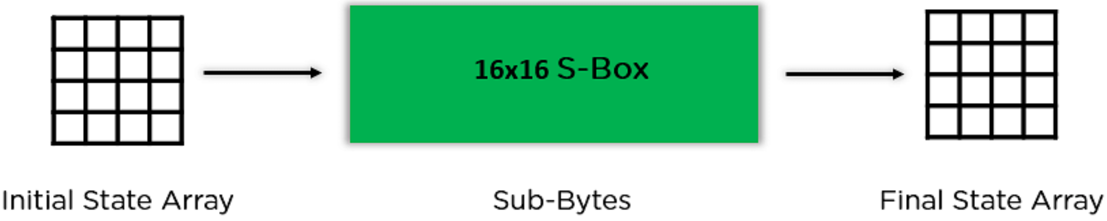
- **Add Round Key:** You pass the block data stored in the state array through an XOR function with the first key generated (K0). It passes the resultant state array on as input to the next step.



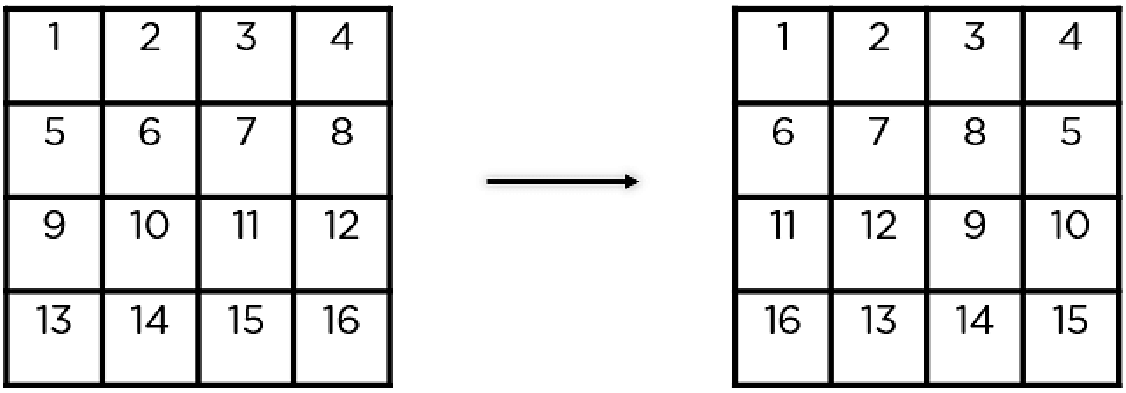
1	2	3	4
6	7	8	5
11	12	9	10
16	13	14	15

K_0	K_1	K_2	K_3
K_4	K_5	K_6	K_7
K_8	K_9	K_{10}	K_{11}
K_{12}	K_{13}	K_{14}	K_{15}

- **Sub-Bytes:** In this step, it converts each byte of the state array into hexadecimal, divided into two equal parts. These parts are the rows and columns, mapped with a substitution box (S-Box) to generate new values for the final state array.



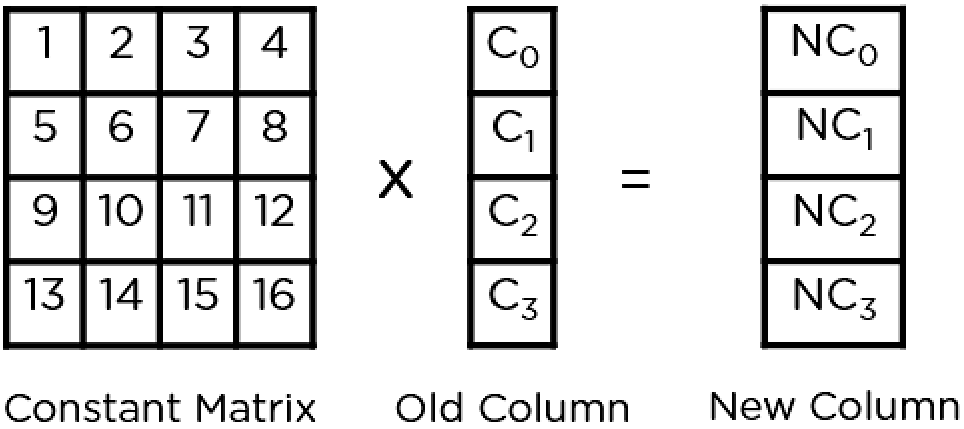
- **Shift Rows:** It swaps the row elements among each other. It skips the first row. It shifts the elements in the second row, one position to the left. It also shifts the elements from the third row two consecutive positions to the left, and it shifts the last row three positions to the left.



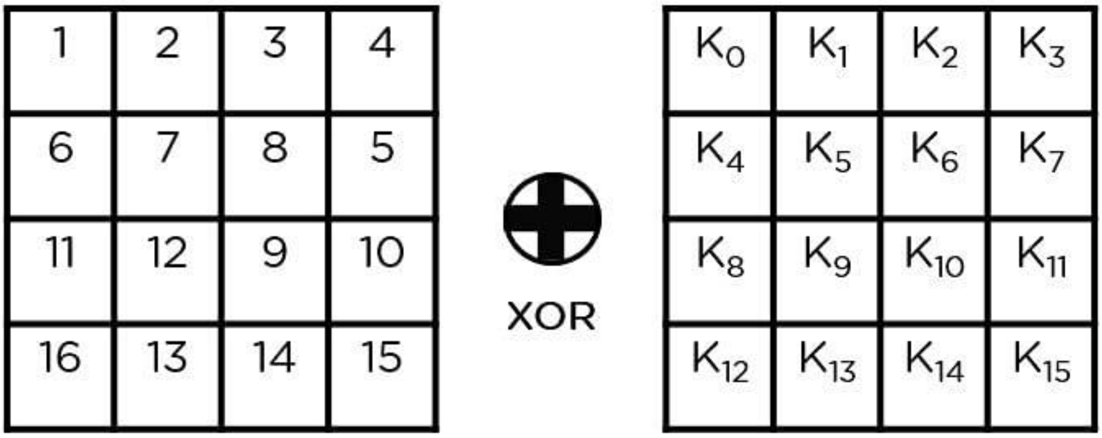
1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

1	2	3	4
6	7	8	5
11	12	9	10
16	13	14	15

- **Mix Columns:** It multiplies a constant matrix with each column in the state array to get a new column for the subsequent state array. Once all the columns are multiplied with the same constant matrix, you get your state array for the next step. This particular step is not to be done in the last round.

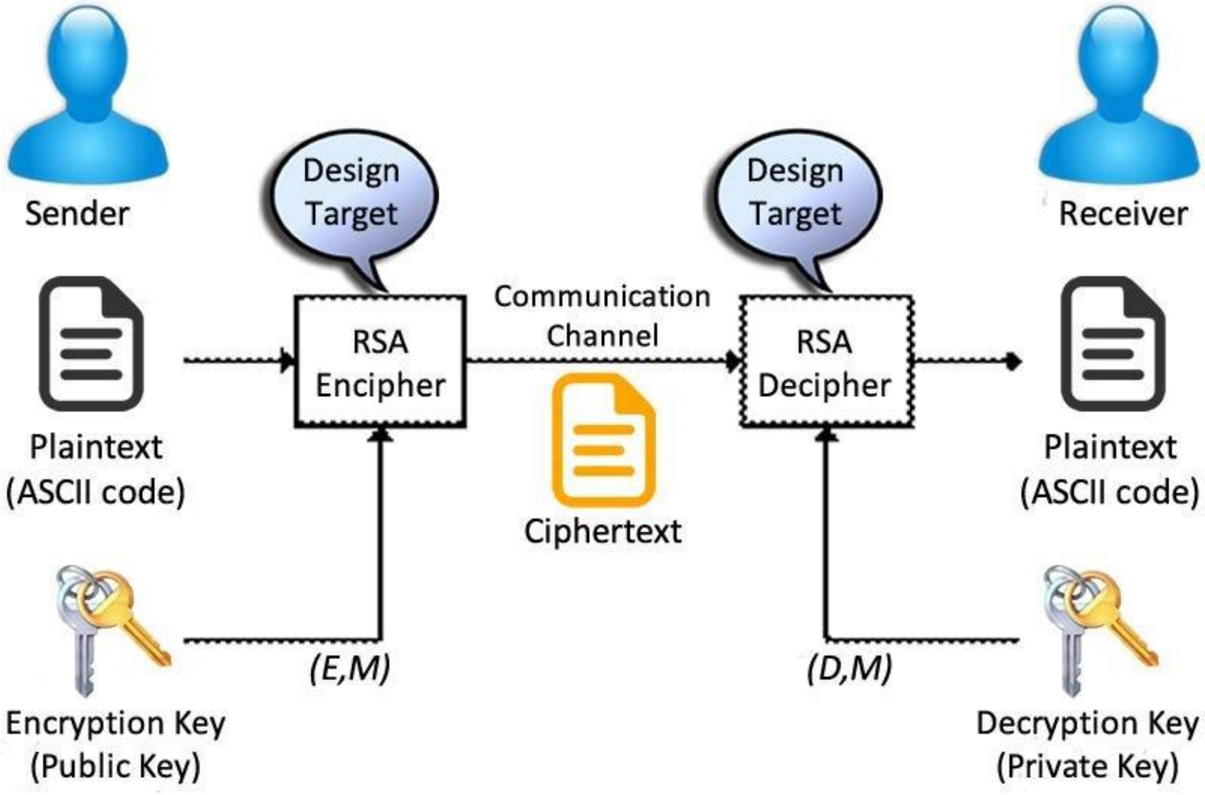


- **Add Round Key:** The respective key for the round is XOR’D with the state array is obtained in the previous step. If this is the last round, the resultant state array becomes the ciphertext for the specific block; else, it passes as the new state array input for the next round.



Rivest, Shamir, and Adleman(RSA) Algorithm

RSA is a commonly adopted public key cryptography algorithm. The first, and still most commonly used asymmetric algorithm RSA is named for the three mathematicians who developed it, Rivest, Shamir, and Adleman. RSA today is used in hundreds of software products and can be used for key exchange, digital signatures, or encryption of small blocks of data. RSA uses a variable size encryption block and a variable size key. The keypair is derived from a very large number, n, that is the product of two prime numbers chosen according to special rules. Since it was introduced in 1977, RSA has been widely used for establishing secure communication channels and for authentication the identity of service provider over insecure communication medium. In the authentication scheme, the server implements public key authentication with client by signing a unique message from the client with its private key, thus creating what is called a digital signature. The signature is then returned to the client, which verifies it using the server's known public key [9]. Encryption algorithms consume a significant amount of computing resources such as CPU time, memory, and battery power. This paper examines a method for evaluation performance of various algorithms. A performance characteristic typically depends on both the encryption key and the input data. A comparative analysis is performed for those encryption algorithms at different sizes of data blocks, finally encryption/decryption speed.



Experimental Design

The five text files of different sizes are used to conduct five experiments, where a comparison of three algorithms AES, DES and RSA is performed. A cryptography too is use to conduct experiments.

Evaluation Parameters

Performance of encryption algorithm is evaluated considering the following parameters.

A. Computation Time

B. Memory usage

C. Output Bytes

The encryption time is considered the time that an encryption algorithm takes to produces a cipher text from a plain text. Encryption time is used to calculate the throughput of an encryption scheme, is calculated as the total plaintext in bytes encrypted divided by the encryption time. Comparisons analyses of the results of the selected different encryption scheme are performed.

Experimental Results and Analysis

Experimental result for Encryption algorithm AES, DES and RSA are shown in table1, which shows the comparison of three algorithm AES, DES and RSA using same text file for five experiment, output byte for AES and DES is same for different sizes of files.

By analyzing the table 1, we noticed the RSA has very smaller output byte compare to AES and DES algorithm. Time taken by RSA algorithm is much higher compare to the time taken by AES and DES algorithm. Variation in memory usage is noticed. It does not increase according to size of file in all algorithms.

By analyzing Fig. one which shows time Taken for encryption on various size of text file by three algorithms i:e AES, DES and RSA, it is noticed that RSA algorithm takes much longer time compare to time taken by AES and DES algorithm . DES algorithm consumes least time for encryption. AES and DES algorithm show very minor difference in time taken for encryption.

Fig. 3 shows the size of output byte for each algorithm used in experiment. The result of Fig. shows same size of output byte for different size of text file in case of all three algorithms.

Table 1: Comparisons of AES, DES and RSA of Time, Memory and Output byte.

DATA	ALGO.	TIME (SEC)	MEMORY (KB)	OUTPUT BYTE
FILE 1 (68KB)	AES	2.2	81,912	131,072
	DES	1.8	85,261	131,072
	RSA	9.4	91,814	65,536
FILE 2 (105)	AES	2.1	62,544	131,072
	DES	1.8	67,531	131,072
	RSA	10.5	77,117	65,536
FILE 3 (124 KB)	AES	2.2	53,902	131,072
	DES	2	55,395	131,072
	RSA	11.4	57,178	65,536
FILE 4 (235KB)	AES	2.4	16,679	131,072
	DES	2.1	21,189	131,072
	RSA	16.2	26,891	65,536
FILE 5 (435KB)	AES	2.6	34,207	131,072
	DES	2.4	42,113	131,072
	RSA	24.4	44,321	65,536

Fig. 1: Comparison of Computation Time among AES, DES and RSA

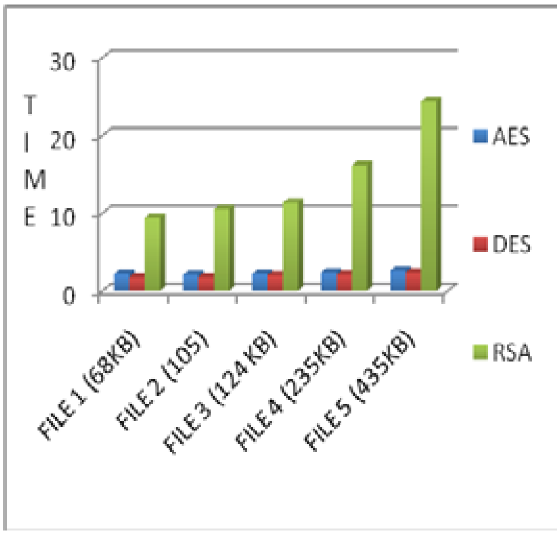


Fig. 2: Comparison of Memory usage by AES, DES and RSA

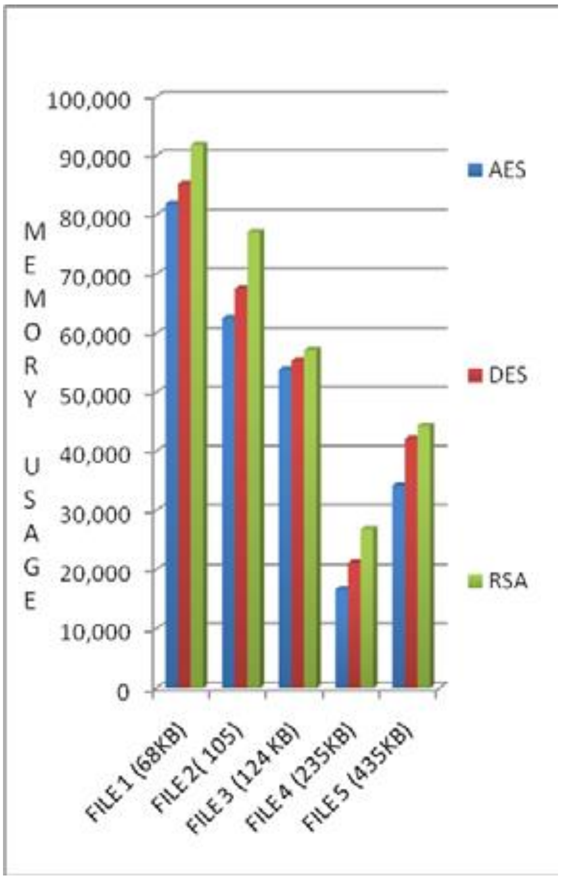
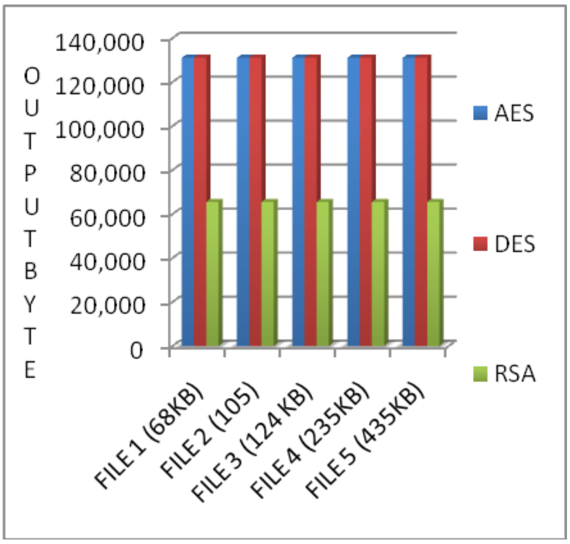


Fig. 3: Comparison of Output Byte used by AES, DES and RSA



Encryption algorithm play an important role in communication security where encryption time, Memory usages output byte and battery power are the major issue of concern. The selected encryption AES, DES and RSA algorithms are used for performance evaluation.

Based on the text files used and the experimental result it was concluded that DES algorithm consumes least encryption time and AES algorithm has least memory usage while encryption time difference is very minor in case of AES algorithm and DES algorithm.

RSA consume longest encryption time and memory usage is also very high but output byte is least in case of RSA algorithm.

Our future work will include experiments on image and audio data and focus will be to improve encryption time and less memory usage.