

simply

Endless path to endless erudition



Cyber Security



Estd. 2001

In pursuit of truth, Infinity and beyond...

Department of Computer Engineering

Computer Engineering Department

VISION

“To become a department of national relevance in the field of Computer Engineering.”

MISSION

The Department of Computer Engineering is committed to nurture students with sound engineering knowledge in the field of computing through the effective use of modern tools with a focus on global employability by imbibing leadership qualities, ethical attitude, lifelong learning and social sensitivity.

PROGRAMME EDUCATIONAL OBJECTIVES (PEOs)

PEO 1: Attain Sound Engineering knowledge and use of modern tools effectively to solve real life problems (KNOWLEDGE)

PEO 2: Attain need based skills and life long learning to ensure global employability (SKILL)

PEO 3: Become successful professionals and responsible citizens with good leadership qualities and strong ethical values (PROFESSIONALISM)

PROGRAMME OUTCOMES (Pos)

PO 1: **ENGINEERING KNOWLEDGE:** Apply Knowledge of Mathematics, Science, engineering fundamentals and an engineering specialization to the solution of complex engineering problems.

PO 2: **PROBLEM ANALYSIS:** Identify, Formulate, Research Literature and Analyze Complex engineering problems reaching substantiated conclusions using first principles of mathematics, natural sciences and engineering sciences.

PO 3: **DESIGN / DEVELOPMENT OF SOLUTIONS:** Design solutions for complex engineering problems and design system components or processes that meet specified needs with appropriate consideration for public health and safety, cultural, societal and environmental considerations.

PO 4: **CONDUCT INVESTIGATIONS OF COMPLEX PROBLEMS:** Using research based knowledge and research methods including design of experiments, analysis and interpretation of data and synthesis of information to provide valid conclusions.

PO 5: **MODERN TOOL USAGE:** Create, select and apply appropriate techniques, resources and modern engineering and IT tools including prediction and modelling to complex engineering activities with an understanding of limitations.

PO 6: **THE ENGINEER AND SOCIETY:** Apply reasoning informed by contextual knowledge to assess societal, health, safety, legal and cultural issues and the consequent responsibilities relevant to professional engineering practice.

PO 7: **ENVIRONMENT AND SUSTAINABILITY:** Understand the impact of professional engineering solutions in societal and environmental contexts and demonstrate knowledge of and need for sustainable development.

PO 8: **ETHICS:** Apply ethical principles and commit to professional ethics and responsibilities and norms of engineering practices.

PO 9: **INDIVIDUAL AND TEAM WORK:** Function effectively as an individual, and as a member of leader in diverse teams and in multi-disciplinary settings.

PO 10: **COMMUNICATION:** Communicate effectively on complex engineering activities with the engineering community and with society at large, such as being able to comprehend and write effective reports and design documentation, make effective presentations, and give and receive clear instructions.

PO 11: **LIFE-LONG LEARNING:** Recognize the need for and have the preparation and ability to engage in independent and life-long learning in the broadest context of technological change.

PO 12: **PROJECT MANAGEMENT & FINANCE:** Demonstrate knowledge and understanding of engineering and management and leaders in a team to manage projects and in multidisciplinary environments.

PROGRAM SPECIFIC OUTCOMES (PSO)

PSO 1: Develop academic aptitude and apply knowledge of computing and mathematics to computer science problems and thereby design and develop Software and Hardware Systems.

PSO 2: Enhance research skills and utilize advanced computing tools for analysis, design and implementation of computing systems for resolving real life / social problems.

PSO 3: Utilize multi-disciplinary knowledge required for satisfying industry / global requirements and hence develop an attitude for life long learning.

PSO 4: Have all round personality with skills like leadership, verbal and written communication, team work, sensitivity towards society in order to become valued and responsible professionals.



Editorial Committee

Editing

Mrinal Bageshwari (TE CMPN A)

Tejas Gupta (TE CMPN A)

Athashree Vartak(SE CMPN B)

Saurabh Jha(SE CMPN A)

Art Design

Sagar Pathare(TE CMPN B)

Adit Rathi(SE CMPN B)

Faculty Members

Dr. Sheetal Rathi, HOD CMPN

Ms. Harshala Yadav, A.P. CMPN

Mrs. Ashwini Patil, A.P. CMPN



Dean's Message

It's the hardwork that has brought this journey a success over the years. I take pride in announcing the release of the sixth edition of the Nimbus magazine. Nimbus has not only proved out to be the best platform for TCET's Computer Department students to showcase their technical knowledge but also their skills of penmanship.

The magazine allows students to share their knowledge and ideas in this crpyted field of technology and engineering with focus on industry/research areas. Our institute aims at promoting- writing and publishing skills of students. This helps the students in expressing their ideas in a very persuasive and expressive manner. Gladly, we have turned this into reality through our initiative.

I would like to congratulate students, teachers and everybody else involved in who took this opportunity thereby building the soul of Nimbus.

Wishing everyone loads of success.

Dr. R. R. Sedamkar



HOD's Message

The passion to explore, innovate and contribute prevails among the students of TCET and NIMBUS is a reflection of that zeal. Our objective through the departmental magazine is to provide a platform for the students and staff to transcribe their ideas and research so as to contribute to the technical knowledge of the readers.

In this edition, we destine to throw light on the topic of "Cyber Security". We hope that the readers of 6 th edition of Nimbus, will be able to absorb all that we wish to convey while we've compiled this issue, considering the hard work and efforts put in by all the stakeholders of the department viz. students, the magazine committee, teachers and industry experts.

Congratulations to the committee and the writers for their praiseworthy contribution. Thank you for your valuable time and efforts worthy of note.

Dr. Sheetal Rath



Faculty Incharge's message

In the previous editions of Nimbus we've seen topics like an engineer's traits,..... In this edition we'll take a look at the contemporary emerging challenge of cyber security.

Cyber security is one of the top concerns in today's world as the world grows digitally. In this edition, we explore topics that have had huge impacts in everyone's lives. Living in a progressively networked world - from personal banking to government infrastructure, protecting networks has become crucial. We have outlined several threats to cyber security - and the steps to be taken to generate awareness.

Thanks to all our well wishers, and writers for sending us articles. Let me present you with our sixth edition of NIMBUS - "Cyber Security".

Best wishes to all.

Ms. Harshala Yadav



FROM THE EDITORS' DESK

At the very beginning we would like to extend our unfeigned gratitude to our Principal Dr. B K Mishra, our Dean-Academics Dr. R R Sedamkar and our Head of Department Dr. Sheetal Rathie for their inspiration and prolific motivation towards the working of this issue of Nimbus.

Being a part of Team Nimbus for the last 4 editions we have seen the journey of this magazine from being a collection of some articles to a magazine that involves all the stakeholders of the course. In this pursuit of knowledge, we have covered many aspects of the field of computer sciences which have proven to be helpful to our readers to understand new concepts and think in a new direction with positive intent altogether.

This edition is aimed at educating engineers about the growing field of CYBER SECURITY, and how technology is being used for its implementation, thus developing insights in those areas that are not extensively taught in constraint to the syllabus. Topics like Cyber Terrorism, Data Breach, Cryptography, Mobile Protection and many case studies of potential threats and recent attacks are being addressed in this edition.

On a closing note I would give special thanks to the faculty in-charge of this issue Ms. Harshala Yadav for her easy-going support and motivation and our team of editors and designers for their motivated and eager attitude to their work and in making sure, that Nimbus maintains its standard it has set through the previous issues, by bringing in phenomenal content. Without them, this issue would have remained what we dreamt it to be.

Tejas Gupta & Mrinal Bageshwari
Co-Editors

Sagar Pathare
Head Designer

Index

Faculty

Ransomware

Student

An Overview of Cyber Security

Security: An illusion

Recent Infractions in Cyber Security

Cyber Security- The First line of Defence

Data Breach

Network Security & Cryptography

Multilevel Network Security

Security Assessment Model Infrastructure as a Service (IaaS) Clouds

Website Security

Mobile Security

Mobile Forensics

How Password Hashing improves Security

Password Managers

Cyber Terrorism

Cyber Terrorism Cases

Zero day attack

The Latest Global Cyber Attack: Ransomware

Top Ransomware Attacks

Cryptocurrencies

Bitcoin "A Peer-to-Peer Network"

Block Chain

Are we at the verge of a security apocalypse by Artificial Intelligence?

Industry

Career Opportunities in Cyber Security

Achievements

Student Editorial Committee

Acknowledgments



RANSOMWARE

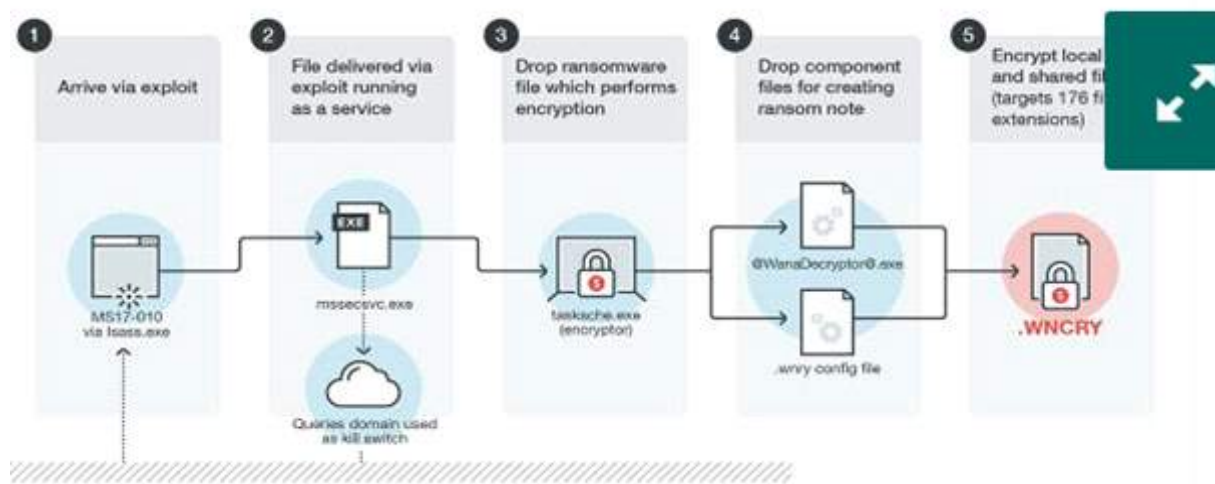
It is a type of malicious software from cryptovirology that is designed and used to threaten the victims to broadcast the data or block access to a computer system until a sum of money is paid. The intention for ransomware attacks is nearly always monetary, and unlike other types of attacks, the victim is usually notified that an attack has occurred and is given instructions for how to recover from the attack. Recovering the files after the attack without the decryption key is an intractable problem and payment is demanded in digital currencies such as Ukash and Bitcoin, which makes tracing and prosecuting the perpetrators difficult.

Ransomware malware is typically carried through malicious email attachments, infected software apps, infected external storage devices and compromised websites that are disguised as a legitimate file that the user is tricked into downloading or opening. In a ransomware attack, the malware may change the victim's login credentials for a computing device; in a data kidnapping attack, the malware may encrypt files on the infected device, as well as other connected network devices.

Examples of ransomware

1. CryptoLocker

Encrypting ransomware was active on the internet from September through May of the following year, which generated a 2048-bit RSA key pair and a security firm gained right of entry to a command-and-control server used by the attack and improved the encryption keys used in the attacks. The malware defenseless to delete the private key if a compensation of Bitcoin or a pre-paid cash voucher was not made within 3 days of the infection. Due to the enormously large key size it uses, analysts and those affected by the Trojan considered CryptoLocker extremely difficult to repair.



2. CryptoWall

CryptoWall first appeared in 2014. One strain of CryptoWall was dispersed as part of an advertising campaign on the Zedo ad network in late-September 2014 that targeted numerous major websites; the ads redirected to crook websites that used browser plugin exploits to download the payload. A Barracuda Networks researcher also distinguished that the payload was signed with a digital signature in an attempt to appear honest to security software. CryptoWall 3.0 used a payload written in JavaScript as part of an email attachment, which downloads executables masquerading as JPG images. To further avoid detection, the malware creates new instances of explorer.exe and svchost.exe to converse with its servers. When encrypting files, the malware also deletes quantity of shadow copies and installs spyware that steals passwords and Bitcoin wallets.

3. WannaCry

WannaCry spread through the Internet, using an exploit vector named EternalBlue was able to infect and encrypt more than 230,000 computers in systems globally and using 20 different languages to demand money from users using Bitcoin cryptocurrency. The malware uses asymmetric encryption so that the victim cannot reasonably be expected to make progress the (private and undistributed) key needed to decrypt the ransomed files.

During the broad of the week in which WannaCry was most dangerous, only about \$100,000 in bitcoin was transferred (to no avail: There are no

accounts of data having been decrypted after payment).

Ransomware prevention

To look after against ransomware attacks and other types of cyberextortion, experts advise users to back up computing devices on a usual basis and update software -- including antivirus software on a regular basis. End users should be aware of clicking on links in emails from strangers or opening email attachments. Victims should do all they can to stay away from paying ransoms. While ransomware attacks may be nearly impossible to stop, there are important data protection proceedings individuals and organizations can take to ensure that harm is minimal and healing is as quick as possible

Gautam Kumar V. Jha
Faculty
CMPT

An Overview of Cyber Security

We have heard of various social crimes but hearing about Cyber Crimes is strange . We install CCTV cameras and other security devices to overcome social crime but what about our activities done on computer ,our browsing datas , etc. are they save? Unfortunately the answer is no. As technology is hitting its target , it is giving rise to various other problems like Cyber Crime. To tackle the problem of Cyber Crime , Cyber Security comes into picture...

Cyber Security is basically set of techniques adapted for protecting computers, networks, programs and data from unauthorized access or attacks that are aimed for exploitation. Major areas covered in cyber security are application security, information security, disaster recovery, network security.

Application security encompasses measures or counter-measures that are taken during the development life-cycle to protect and deal with the threats that can come through flaws in the application design, development, deployment, upgrade or maintenance. Some basic techniques used for application security are input parameter validation , user/role authentication & authorization, session management, parameter manipulation & exception management and auditing and logging.

Information security protects information from any unauthorized access in order to avoid identity theft and to protect privacy . Major techniques used to cover this are identification, authentication & authorization of user , cryptography.

Disaster recovery planning is a process that includes performing risk assessment, establishing priorities, developing recovery strategies in case of a disaster. Any business should have a concrete plan for disaster recovery to resume normal business operation as quickly as possible after any sort of disaster.

Network security includes activities to protect the usability, reliability, integrity and safety of the network. Effective network security targets a variety of threats and thereby prevents them from entering or spreading on the network. Network security components include anti-virus and anti-spyware , firewall, to block unauthorized access to your network , virtual private networks (VPNS), to provide secure remote access .

But at the same time question arises that why cyber security has become an important issue today ..well, it is because we all live in a world which is networked together, from internet banking to government infrastructure, and thus, network protection is no longer an optional extra. Cyber attack is now an international concern, as high-profile breaches have given many concerns that hacks and other security attacks could endanger the global economy. A cyber-attack is a deliberate exploitation of computer systems, technology dependent enterprises and networks. Cyber attackers use malicious code and software to alter computer code, logic, or data, resulting in disruptive consequences that can compromise data and lead to Cyber Crimes such as information and identity theft or system infiltration.

Cyber Crime is unlikely to slow down, despite of constant efforts taken by the government and by the specialists. Its growth is being driven by the expanding number of services available online, and the increasing evolution of online criminals who are engaged in a continuous game with security experts .With constant technical innovation, new dangers are constantly coming to the surface. For instance , the migration of data to third-party cloud providers has created an epicentre of data and therefore, more opportunities to misappropriate critical information from a single target.

Cyber Crime thereby makes Cyber Security to be thorough and seamless, regardless of business size or organizational standing. Computer networks will forever be the target of criminals, and it can be argued that the danger of Cyber Security breaches will only increase in the future as networks continue to expand. It is also very important to impose strict actions by the government if any private data is accessed by any unauthorized user. Having the right level of preparation and specialist assistance is vital to minimize and control damage, and recover from a Cyber breach and its consequences thus cyber security has become an important issue today which is to be taken care of.

Aishwarya Gupta
SE-CMPN-A



Security: An Illusion

WikiLeaks' Vault7 issue of leaked CIA documents specifying its hacking tools discloses malware called OutlawCountry that targets Linux based systems.

OutlawCountry is defined in documents dated June 4, 2015 as a kernel module for Linux 2.6 that permits CIA operators to redirect outbound traffic to the server they control by making a hidden netfilter or iptables table. Netfilter is packet-filtering framework within the Linux kernel's networking stack.

The recent ransomware attack, which affected organizations around the globe including Britain's National Health Service, was the first real illustration. Criminal hackers exploited a fault in 'retired' Microsoft software, which is not regularly updated for safety, to infect computers with the WannaCry ransomware.

But what if devices were even weaker, running with no built-in security and no opportunity to patch? This is the problem that the so-called internet of things (IoT) presents. With an predicted 22.5 billion devices due to be connected to the internet by 2021, the chance for holding these devices to ransom will present significant opportunities to hackers and will have severe consequences for providers and users of these devices.

Last year the huge Distributed Denial of Service (DDoS) attack that brought down the Dyn Domain Name System (DNS) service demonstrated the vulnerability of certain platforms to attacks using the IoT. During that attack the committers managed to deny access to major platforms like Twitter, Netflix and Facebook for some hours. It was made possible through binding poorly protected household devices such as security CCTV and baby monitors which still had the factory password programmed or no built in security.

This attack was significant and cost Dyn clients but it didn't have an effect on infrastructure such as hospitals and doctors' surgeries in the way, current attack has, where denying access to patient records could deferral vital treatment. But the IOT has had and could have further significant physical consequences, even the most placid of objects can be weaponized.

Self-driving cars are already being examined on the streets and it is likely that there will be 10.5 million self-driving cars on the roads by 2021. Self-driving cars are part of the so called Internet of Automotive Things (IoAT), a network of sensors and computer processes that will reduce accidents caused by human mistake and eventually make the roads a safer place. They will also be securely designed and protected with the capacity to cover and update security software but they will not be impervious to hacking.

The advancement in technologies will always help us but will also open new gates to vulnerabilities. Privacy on internet has become myth.



Shivam Mishra
Sharad Bharadia
BE-CMPN-A

Recent Infractions in Cyber Security

Pacemakers:

It is important to know that security against attacks is not only restricted to computers and laptops but to every electronic device. Any device that is remote controlled by can be hacked into. Hacking has developed so much that now not only social media accounts and phones but even pacemakers are being hacked! And not only pacemakers but defibrillators and insulin pumps too, whose manufacturers increasingly are loading them with software updates to improve performance and secure the instruments.

Around 465,000 Americans with pacemakers fitted were advised to visit their doctor to get an important software upgrade – otherwise their life-saving inner gadget could be vulnerable to a hacking attempt. These artificial pacemakers are fitted with tiny radio components so they can be controlled and updated without having to cut them out and replace them each time. However, the flaw discovered in the faulty pacemakers means someone with the right technical know-how could connect to one of the devices and change its settings – maybe even stopping it altogether.

That might seem extreme, but it's not all that difficult to do, and security researchers have raised the possibility of someone using this as a way of extorting money. In 2015, a group of researchers from university of South Alabama hacked a pacemaker and killed a person in iStan stimulator. The \$100,000 iStan has “internal robotics that mimic human cardiovascular, respiratory and neurological systems. When iStan bleeds, his blood pressure, heart rate and other clinical signs change automatically.”

Why should anyone care that a simulated human can be hacked? Because of the dreaded ripple effect. According to the researchers, “If medical training environments are breached, the long term ripple effect on the medical profession, potentially, impacts thousands of lives due to incorrect analysis of life threatening critical data by medical personnel.”

In its report, the FDA didn't shy away from painting a horror scenario, one in which a researcher notifies a manufacturer that its implantable device “can be reprogrammed by an unauthorized user.” “If exploited, this vulnerability could result in permanent impairment, a life-threatening injury, or death,” according to the FDA.

NASA

According to Gray McKinnon, a man who somehow managed to hack into NASA and U.S. Nav computers, all statements from different people about secretive space programs, highly classified technologies, and even alien life are correct. Between February 2001 and March 2002 Gary McKinnon, who was initially looking for evidence of free energy suppression and a cover-up of UFO activity and other technologies potentially useful to the public, hacked into 16 NASA computers as well as dozens of US Army, Navy, Air Force, and Department of Defence computers. Gary McKinnon—the man who hacked NASA—firmly stated that he uncovered evidence that the United States has a fully operational fleet of Space Warships. In a new interview on UFO channel Richplanet TV. McKinnon finally revealed the entire truth about his findings saying: ‘I kept going for months and months. I kept thinking, ‘They’re going to close this door’. I scanned and looked for documents, I found an Excel spreadsheet which said, ‘Non-terrestrial officers’, states McKinnon. Gary McKinnon is accused of mounting the biggest ever hack in the history of the United States by breaking into the computers of the Army, Air force, Navy and NASA. Furthermore, the NASA hacker claimed that he uncovered around 25 rows of details of officers’ ranks, names and ships accordingly. Some would say it’s all a massive conspiracy, and quotes, information and declassified documents were taken out of context but, the truth is that there is plenty of stuff which makes it hard to tell.

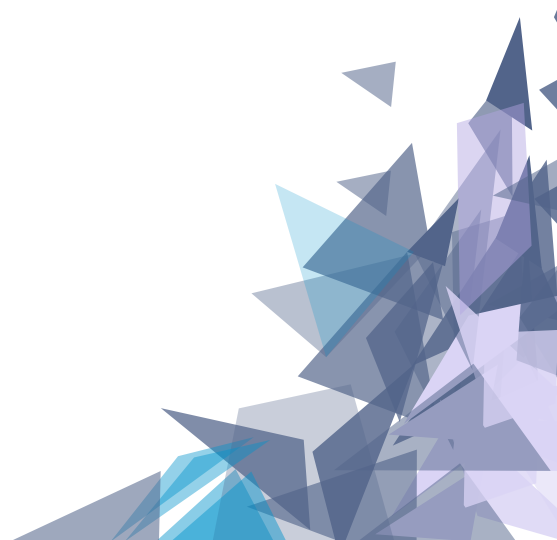
HBO

One of the most recent cyber attacks on July 31, 2017 news broke that HBO had experienced a major cyberattack. As first reported by Entertainment Weekly, the hackers who executed the attack claimed to have acquired 1.5 terabytes of data from the network — allegedly including scripts and other content for the network’s marquee series, Game of Thrones. The hackers made it one of their first orders of business to release unaired episodes of Ballers and Room 104 online. But they didn’t stop there, sending a cryptic and oddly worded email several to different members of the media

that read “Hi to all mankind. The greatest leak of cyber space era is happening. What’s its name? Oh I forget to tell. Its HBO and Game of Thrones.....!!!!!! You are lucky to be the first pioneers to witness and download the leak. Enjoy it & spread the words. Whoever spreads well, we will have an interview with him. HBO is falling.” HBO has confirmed that a cyberattack took place, both to news outlets and in internal statements. But if the hackers’ claim of stealing 1.5 terabytes of raw data is accurate, the HBO hack is roughly seven times larger than the 2014 Sony hack, which involved roughly 200 gigabytes of data. On August 3, someone going by the name of “Kind Mr. Smith,” who claimed to have been involved the attack, sent an email to an unknown list of recipients that included the Hollywood Reporter. ‘HBO is Bluffing. We STILL have full access to their webmails....’, the email said, apparently commenting on CEO Richard Plepler’s email to HBO employees. The email claimed that “Kind Mr. Smith” had “weeks” of negotiations with HBO regarding the stolen information. “They broke their promises and want to play with us,” the email says. It is unconfirmed as to whether the sender was indeed involved in the hack, but some have noted that the email is written in the same caustic tone as the original message sent to select press, which feels like something out of an early 2000s hacker film.

Cyber crime is estimated to be worth £34 billion a year. Six million people have fallen victim to it in the past year, with 1.4 million reporting computer virus attacks, and 650,000 emails and social media profiles stolen. You can never make any system full proof but the plan is to stay one step ahead of the attackers.

Suchit Gupta
SE-CMPN-A





Cyber Security- The First line of Defence

Cyberspace, a domain created by The Human, not by nature and it has evolved to provide tremendous benefits, but also to present new risks. Cyber security has become a national policy issue, democracies have formulated several national Cyber strategies. As we have progressed to embedded systems of Inter-connected information technology, the whole network is getting more and more prone to attacks causing data theft, manipulation it to create confusion in the network. Cyber warfare is the ultimate motive behind these Cyber-attacks, as all of them focused on crime, terrorism, industrial espionage, military espionage, or warfare.

Cyber warfare is Internet-based conflict politically motivated attack on information systems. Cyber warfare attacks can disable official websites and networks, disrupt or disable essential services, steal or alter classified data, and cripple financial systems. Every year a Cyber war is held on 14th and 15th August as a celebration of Independence Day between the hackers of India and Pakistan, with a motive to hack major government sites of the other nation. The definition of Cyber Warfare is purely emerged from the conditions behind war. After World War II, the whole world fear that the next war will be an atomic one but the war has already started and it is Cyber war as all the nations are trying to get the confidential data of the rival nations to get an insight of their weak spots. The challenge in cyber security is that the initial phases of an attack, such as malware or spear-phishing emails, vary every time and the attack is launched, making it impossible to detect and classify the malicious programs. (This is another way of restating the famous mathematical proof attributed to Alan Turing in the 1930s of the so-called halting problem. In this case, it's impossible for a computer program to determine whether another program is good or bad.)

Technologies like Artificial Intelligence are being developed for security purposes as there has been an increase in automated and sophisticated social engineering attacks and in no time the attackers will switch to AI-enabled hacking and the only way to tackle them is by the AI-based defensive firewall systems. While AI is a technology with an ability to improve itself based on the performance, but the current development of AI is not even close to that stage. A better available option is by Machine Learning (ML).

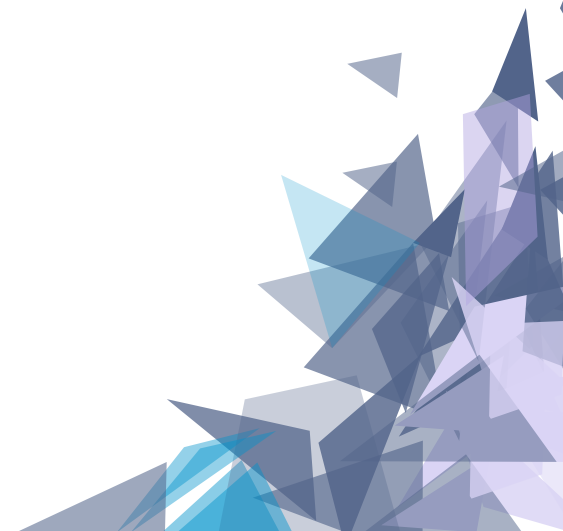
It is a sub-field of computer science which helps a computer learn and decide how to behave with the given set of inputs, without being implicitly programmed and ML will also facilitate the Security of the systems with the techniques overlapping with mathematical optimization and data mining. ML basically uses algorithms that can learn from data. With good training data, ML algorithms can do a pretty good job of training a model that can then be used to sift through new, unlabeled data.

Internet of Things (IoT – The next Trojan Horse): IoT the most emerging technology behind automation has now become a nightmare for the corporates using it as the hackers are using IoT as a Trojan Horse to get into the system easily as the IoT devices come protected with the default passwords for the convenience of the users but they bring vulnerability to the network. The attacks by an IoT device is by using the coded signals of the IR-remote keys to unlock the car. Car's IR-keys use rolling codes for the commands to prevent copying of the remote's code to create a dummy remote but as AI systems are used for security against AI-enabled hacking, similarly an IoT device is used to intrude the codes of the IR-keys as the auto makers don't set an expiry date for the rolling code sent to the car, so even if a single code cannot be used twice but what if it doesn't reach the car. This wallet-sized device is hidden on or underneath the target car. As the unlock key is pressed this device catches the signal and jams it, since the car has not received the signal the owner sends the signal again. This time the Rolljam device records and jams the signal and sends the previous code storing one code for the intruder.

IoT controlled appliances are the most vulnerable to the safety as every company sets a sequence to pattern to reprogram the controller of the appliances, this code makes the controller scan all the devices in the vicinity and the command will be compatible with the device all you need is to get a controller of the same enterprise. Similarly the automations implemented on large scale can be hacked over the Internet easily and make you defenseless in your own house.

Military organizations have started using drones rather than sending teams in the enemy territory similar to the Greek's Trojan horse used to win the city of Troy." On the other hand there is a particular urgency because the merger of physical and digital domains in IoT are increasing the consequences of cyberattacks. In 10-15 years, we will be deep in a war of the machines' an era with advanced artificial intelligence bringing a battle of AI vs AI. The availability of low cost computing and storage, off-the-shelf machine learning algorithms, AI code and open AI platforms will drive increased AI use by the good guys to defend and protect – but also increase deployment of AI by the bad guys. There will be sophisticated attacks launched on a grand scale, quickly and intelligently with little human intervention, that compromise our digital devices and web infrastructure. Cybercriminals will create fully autonomous, AI-based attacks that will operate completely independently, adapt, make decisions on their own and more. Security companies will counter this by developing and deploying AI-based defensive systems. Humans will simply supervise the process.

Agrim Singh
BE CMPN B



Data Breach

The world has come to a point where every individual has become desensitized with the news of a data breach. Every now and then, companies announce that their systems were breached, followed by the extent of the damage, and what they are doing about it. Data breaches have resulted in millions of private records and sensitive data being stolen, affecting not just the breached organization, but also everyone whose personal information may have been stolen.

WHAT IS DATA BREACH?

A data breach is a phenomena when a cybercriminal successfully infiltrates a data source and extracts sensitive information. This can be done physically by accessing a computer or network to steal local files, or by bypassing network security remotely. Payment data, authentication details, copyrighted materials, medical records, classified information, these are the types of data which are usually stolen.

HOW DOES IT OCCURS?

1. Insider leak: A trusted individual or person of authority with access privileges steals data.
2. Payment card fraud: Credit card/Debit card stolen using physical skimming devices.
3. Loss or theft: Portable drives, laptops, office computers, files, and other physical properties are lost or stolen.
4. Unintended disclosure: Through mistakes or negligence, sensitive data is exposed.



Oh No,
I Lost My Data



There have been various attacks on corporate world causing tons of information leaking. In recent years, companies like Myspace, Tumblr, LinkedIn fell prey to cyber-attacks, causing data breach of almost 1 lac users. In 2015, Anthem, a healthcare company was attacked by hackers, which caused them a loss of almost 80000000 patients, which is considered to be the biggest data breach in last decade. Ubisoft, a gaming company, was also under attack in the year 2013. They lost data for almost 58000000 users. We can see that, despite being the biggest companies of the corporate world, they were still attacked and their data was breached. So, its important for common people to protect their data and not fall prey to the hackers out there.

HOW TO PROTECT YOUR DATA?

- Do not open emails from unfamiliar senders.
- Make use of different and strong passwords. Don't use birthdates, or simple sequential passwords as they are very common and very well known to hackers.
- Think before you post something on social media.
- Protect your credit card/debit card details especially the CVV.
- Make sure you shop from trusted websites. Don't fall prey to phishing pages.



Kevin Shah
SE-CMPN-B

Network Security & Cryptography

Network Security & Cryptography is a concept to protect network and data transmission over wireless network. Data Security is the main aspect of secure data transmission over unreliable network. Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs conducting transactions and communications among businesses, government agencies and individuals.

INTRODUCTION

Network Security is the most vital component in information security because it is responsible for securing all information passed through networked computers. Network security problems can be divided roughly into four closely intertwined areas: authentication, nonrepudiation, integrity control, and confidentiality.

Cryptography is an emerging technology, which is important for network security. The widespread use of computerized data storage, processing and transmission makes sensitive, valuable and personal information vulnerable to unauthorized access while in storage or transmission. Cryptography is a vital of today's computer and communications networks, protecting everything from business e-mail to bank transactions and internet shopping. While classical and modern cryptography employ various mathematical techniques to avoid eavesdroppers from learning the contents of encrypted messages. Computer systems and networks which are storing, processing and communicating sensitive or valuable information require protection against such unauthorized access.

Working

Cryptography provides for secure communication in the presence of third-parties known as adversaries. Encryption a major component of cryptography uses an algorithm and a key to transform an input i.e. plaintext into an encrypted output i.e. ciphertext. A given algorithm will always transform the same plaintext into the same ciphertext if the same key is used. Decryption algorithm used to recover plaintext from ciphertext.

Cryptographic Principles

Redundancy:

The first principle is that all encrypted messages must contain some redundancy, that is, information not needed to understand the message. Messages must contain some redundancy.

Freshness:

Some method is needed to foil replay attacks. One such measure is including in every message a timestamp valid only for, say, 10 seconds. The receiver can then just keep messages around for 10 seconds, to compare newly arrived messages to previous ones to filter out duplicates. Messages older than 10 seconds can be thrown out, since any replays sent more than 10 seconds later will be rejected as too old.

Network Security is the most vital component in information security because it is responsible for securing all information passed through networked computers. Network Security & Cryptography is a concept to protect network and data transmission over wireless network. Network for banking, shopping, inventory control, benefit .The information security can be easily achieved by using Cryptography technique.

Akshata Hirve
TE-CMPN-B

Multilevel Network Security

INTRODUCTION:-

The demand for protecting the privacy and the integrity of messages for communication network has been on the increase in recent years. When a set of computers is interconnected to form a network, the protection mechanisms acting within the individual computers that prevent unauthorized access to the files and illegal flow of information between files stored within these computers become inadequate to ensure the security of inter process of communications across the entire network. Hence a security enforcement mechanism for the network is required in addition to the existing protection mechanisms within the individual computers.

Multilevel Security Policy:-

SE Linux uses the Bell-La Padula BLP model, with Type Enforcement for integrity. In simple terms, MLS policy ensures that a Subject has an appropriate clearance to access an Object of a particular classification. For example, under multilevel security, the system needs to know how to process a request such as: Can a process running with a clearance of write to a file classified. The multilevel security model and the policy implemented for it will determine the answer. Multilevel security meets a very narrow set of security requirements based around the way information and personnel are managed in rigidly controlled environments such as the military. Multilevel security is typically difficult to work with and does not obtain well to general case scenarios. Type Enforcement under SE Linux is a more flexible and expressive security scheme, which is in many cases more suitable than multilevel security. There are several scenarios where traditional multilevel security is still required. For example, if a file server where the stored data may be of mixed classification and where clients connect at different clearances. This will result in a large number of security levels and a need for strong isolation all in a single system. This is the one of the reason that SE Linux includes multilevel security as a security model.



Security Assessment Model Infrastructure as a Service (IaaS) Clouds

The vulnerability of cloud computing systems (CCSs) to advanced persistent threats (APTs) is a significant concern to government and industry. This is a cloud security assessment model that estimates high level security metrics to quantify the degree of confidentiality and integrity offered by a CCS or cloud service provider (CSP). This could be used to assess the security level of four multi-tenant IaaS cloud architectures equipped with alternative cloud security controls

Virtualization, the basis for most CCSs, enables CSPs to start, stop, move, and restart computing workloads on demand. VMs run on computing hardware that may be shared by cloud tenants.

Physical & Virtual trust zones: We define a trust zone as a combination of network segmentation and identity and access management (IAM) controls. These define physical, logical, or virtual boundaries around network resources. Trust zones can be implemented using physical devices, virtually using virtual firewall and switching applications, or using both physical and virtual appliances.

To simplify the analysis we assume all nodes in each node class are identical in terms of their security properties (before any malware is introduced we assume they are identically configured and that if there are system or node configuration errors these are common across all nodes in a node class). Therefore, it is not essential to distinguish between individual elements in each node class, and we can define a Bayesian network model in which the nodes of the network are CCS node classes, and not individual system components of the CCS. This Bayesian network model forms the basis of this model.

We apply Bayesian network statistics to the attack paths described above. Attack paths have been used to understand the vulnerability status of information systems. They have also been used to develop probabilistic measures of enterprise network security.

CCS attack paths: CCS attacks can be divided into outsider or insider attacks. Outsiders can gain access to the cloud using three attack paths:

- (1) exploits weaknesses in cloud access control mechanisms.
- (2) starts by stealing valid credentials of a cloud user at some location outside the cloud (for example from a host inside a government agency).
- (3) outsider attack path starts with the attacker using valid credentials and prior legitimate access to the cloud. When the attacker already exploits credentials for at least one cloud TZ the insider attacks starts, for example the CSP TZ.

This relies on conditional probabilities that represent the probability that a vulnerability in an individual CCS component can be exploited by an APT, if other CCS components have already been compromised.

Here a security model is demonstrated can assess the security status of IaaS CCSs and IaaS CSP service offerings, and be used to estimate probabilities of APT infiltration and detection. These quantify two key high level security metrics: IaaS CCS confidentiality and integrity. Cloud-Trust can also quantify the value of specific CCS security controls (including optional security features offered by leading commercial CSPs). When there is uncertainty regarding the value of a specific security control (which may be optional and increase the cost of CSP services, or which may not be required by industry or government standards).

The scope of this model is currently limited to IaaS CCSs and CSPs. It also does not include all possible insider attack vectors and methods. Possible next steps are to extend Cloud-Trust to include the full range of insider attacks, and to platform as a service (PaaS) and software as a service (SaaS) CSPs.

Raj Shah
TE-CMPN-B





Website Security

Cybersecurity is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access. According to Forbes nearly 30,000 new websites are hacked daily.

Major Threats and Vulnerabilities:

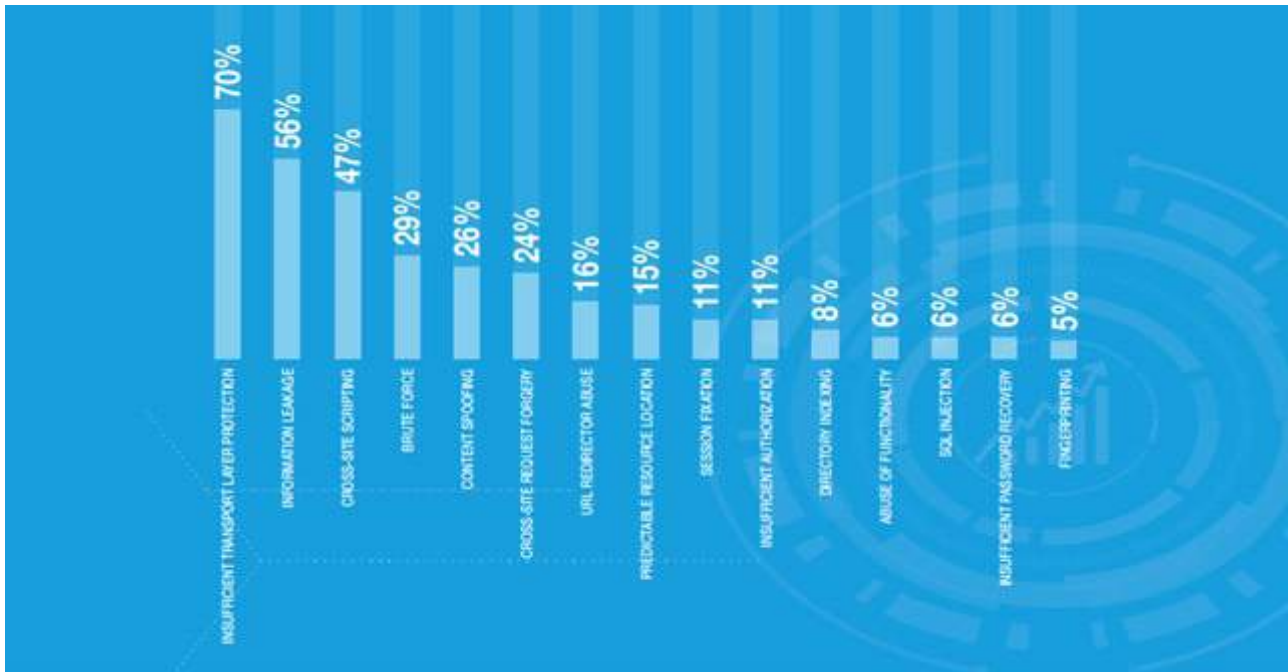
- **Malware** Malware is an abbreviated term meaning "malicious software". This is software that is specifically designed to gain access or damage a computer without the knowledge of the owner.
- **Distributed Denial of Service (DDoS)** A Distributed Denial of Service (DDoS) attack is an attempt to make an online service unavailable by overwhelming it with traffic from multiple sources.
- Also there are several other threats such as Phishing, Sniffing, SQL injection, keyloggers, rootkits.

Protection from Attacks

The best protection from malware continues to be the usual advice: be careful about what email attachments you open, be cautious when surfing and stay away from suspicious websites, and install and maintain an updated, quality antivirus program.

For preventing DDoS, the best way is to

1. Rate limit your router to prevent your Web server being overwhelmed.
2. Add filters to tell your router to drop packets from obvious sources of attack.
3. Drop spoofed or malformed packages.

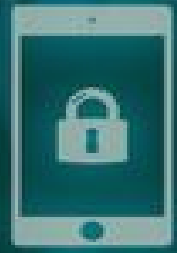


Cybersecurity is a complex subject whose understanding requires knowledge and expertise from multiple disciplines, including but not limited to computer science and information technology, psychology, economics, organizational behavior, political science, engineering, sociology, decision sciences, international relations, and law.

Cybersecurity is a never-ending battle. A permanently decisive solution to the problem will not be found in the foreseeable future.

Nikhil Pandey
Sanjay Varma
TE-CMPN-B

Mobile Security



There are just as many threats on the mobile landscape as there are with desktops and laptops. With the popularity of smartphones and tablets on the rise, they are becoming more of a target to cybercriminals. Since we're starting to use our smaller devices as we would a desktop or laptop computer, more of our personal data is stored on these devices and thieves are taking notice. Learning about the varied types of threats on the mobile landscape and how to stay safe from all of these could be proven beneficial for the individuals. Internet services and websites make it easy for us to pay bills, shop, make online reservations and even work. And these actions can be carried out from any place in the world. Old boundaries and human limitations were dropped, in order for us to have access to almost any information. Our lives became so much easier. But the same thing is true for CRIME. Our freedom to navigate and access a wide number of online locations represents in the same time a main vulnerability to our data, because an open door always allows access in both directions. Criminal minds can reach these days further than before, into our private lives, our homes and work offices. And there is little we can do about it. Attack methods and tools may vary from traditional attack vectors, which use malicious software and vulnerabilities present in almost all the programs and apps (even in the popular Windows operating systems), to ingenious phishing scams deployed from unexpected regions of the world, where justice can't easily reach out to catch the eventual perpetrators.

The most common ways for you to become vulnerable to a malware attack usually happens when you:

- Shop online
- Check your email
- Access social media networks

For this reason, we need to know what are the most popular schemes and techniques used by cyber criminals in order to obtain our private information and financial data. We must not ignore the fact that their final target is always our money and there is nothing they won't do to accomplish their mission.

How to protect yourself?

Have a decent password and use encryption:

Smartphones are physically easier to steal (or lose) than a desktop or laptop computer. Keep your information locked up tight by making use of security options most phones already offer. If your phone is missing, disabling your account by contacting your service provider is the first precautionary step that needs to be taken.

Install necessary updates:

Developers are constantly working to find and remove bugs or other 'holes' that could make your device more vulnerable. Hence, update your device as well as the apps from time to time.

Be a smart 'surfer':

When using the Internet on your phone, prefer secure 'https' sites. Avoid using public Wi-Fi networks when conducting any business that involves finances or other personal information, including login and password information. Turn off WiFi and Bluetooth when you're not using them.

Download with caution:

While apps from Amazon and the iTunes store are relatively safe, the Android Market is rife with malware, and unknown third-party sites can be technological torture. That's because its devices are most common and its development platform is the most open. No matter what device you use, it's a good idea to read reviews of each app you plan to download and pay attention to the permissions it asks for.

Consider security software:

In the next 12 to 18 months it will probably be necessary to install malware protection, especially if you make any kind of financial transactions via your smartphone. Security software will detect and remove viruses, and let you remotely lock or delete data if you lose track of your device.

Siddharth Tiwari
SE-CMPN -B



Mobile Forensics

Why Mobile Forensics?

What's the one thing anybody in the world once used to can't live without? Their Mobile Phones. Mobile devices are an evolving form of computing, used widely in daily life for personal as well as organizational purposes. These devices manage information such as contact information and appointments, corresponding electronically, and conveying electronic documents. Thus, providing ease in maintaining data and documentations ergo increasing individual efficiencies while working on projects. By keeping track of the activities done by the user, the device generates and learns about certain patterns and modules of information. Over time, the devices accumulate a sizeable amount of information about the owner. When involved in crimes or other incidents, proper tools and techniques are needed to recover evidence from such devices and their associated media.

Some important tools to keep handy

EnCase- EnCase is the shared technology within a suite of digital investigations products by Guidance Software. The software comes in several products designed for forensic, cyber security, security analytics, and e- discovery use. Encase is traditionally used in forensics to recover evidence from seized hard drives. Encase allows the investigator to conduct in depth analysis of user files to collect evidence such as documents, pictures, internet history and Windows Registry information.

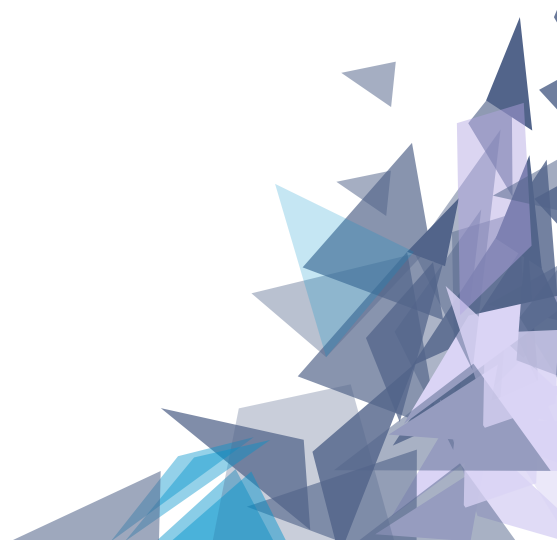
FTK- Forensic Toolkit, or FTK, is a computer forensics software made by AccessData. It scans a hard drive looking for various information. It can, for example, locate deleted emails and scan a disk for text strings to use them as a password dictionary to crack encryption. The toolkit also includes a standalone disk imaging program called FTK Imager. The FTK Imager is a simple but concise tool. It saves an image of a hard disk in one file or in segments that may be later on reconstructed. It calculates MD5 hash values and confirms the integrity of the data before closing the files. The result is an image file(s) that can be saved in several formats, including DD raw.

COFFEE-

Computer Online Forensic Evidence Extractor also said (COFEE) is a tool kit, developed by Microsoft, to help computer forensic investigators extract evidence from a Windows computer. Installed on a USB flash drive or other external disk drive, it acts as an automated forensic tool during a live analysis. Microsoft provides COFEE devices and online technical support free to law enforcement agencies.

Multiple tools are needed to cover the widest range of available mobile phones. Understanding of proper seizure and preservation techniques are paramount. Practice in mock examinations can help gain an in- depth understanding of a tool and subtleties of use, and also provides the opportunity to customize settings for later use. Quality control and tool validation for Mobile Device Forensic tools is significant for proper data acquisition and reporting. This still is a budding sector with lots of promising competition in it will always serve the consumers.

Amey Patil
TE-CMPN-B



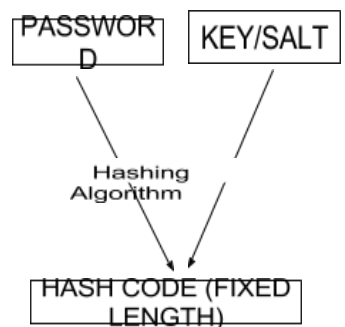
How Password Hashing improves Security

What is Password Hashing?

- Password hashing is used by developers, while making user-account system, to improve security.
- In password hashing, we can convert any password into fixed length code called as hash code, that cannot be reversed.
- In this, certain coding (hashing Algorithm) is done on password (user entered) and key (system generated), to generate a fixed length code, which is stored in database instead of original password.
- Most commonly used hashing algorithms are MD5 and SHA-1.

Why Password Hashing is needed?

- Whenever developer is making user-account systems, most important aspect developer should look upon is how password of user can be protected i.e. password privacy.
- If we store user entered password directly in database, then password is not that secure as user-account database are hacked frequently.
- So, to prevent this, password hashing is used. In this, attacker cannot retrieve password even if he hacks database, as password is stored in form of hashed code.



Work flow in REAL WORLD

- Whenever users set the password of their accounts, password is hashed and stored in database. At no point, unencrypted data is stored.
- Whenever user attempts to login, hash code of password they entered is checked against hash of real password.
- If hash matches with the recorded hash, user is granted access else “invalid password” pops up.

DEVELOPERS LIFELINE!!!

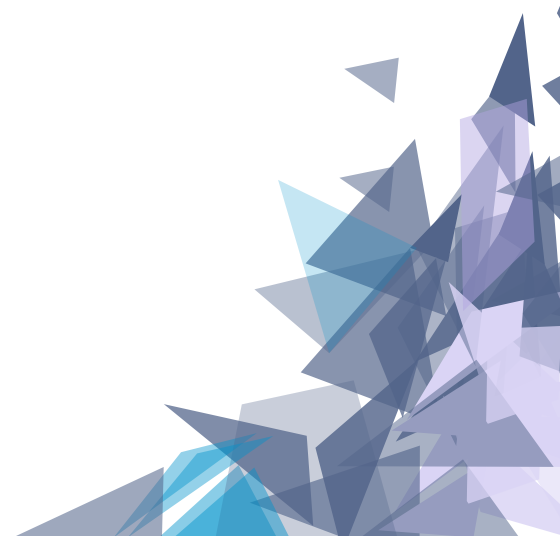
- Value of key should be different for different password. This is necessary because if 2 users having common password will generate same hash code if key remains same. Therefore, key should be generated using CRYPTOGRAPHICALLY SECURE PSEUDO RANDOM NUMBER GENERATOR(CSPRNG).
- Algorithm developed for hashing should be such that hash collisions should be very difficult to find. (hash collision means for different password we get same hash code).
- Key generated should not be too small.
- Well defined key Stretching Algorithms must be used.

Weak Links

- Even if password hashing helps to improve security, original password can be retrieved from hash code using certain methods.
- Two of the most common methods are Brute Force attacks and Rainbow Tables.
- With a Brute Force Attack, attacker will use a piece of software to use every possible combination of character. Software will then use every combination of character in every arrangement until hashcode of it matches with hash code of password. This method is suitable for small and easy passwords. For large password, it takes years to crack.
- Generated collection of hashes and their plaintext equivalent allowing hacker to compare hashed version against stored password hash and identify password are known as Rainbow collections. With rainbow tables, passwords are cracked in small amount of time.
- The smart way to overcome such weak links is by keeping large passwords which includes upper and lower case alphabets, numbers and special characters and changing password frequently.

Today, almost in every user-account system including Yahoo, Facebook, Gmail, etc. hash codes of entered password are stored in database to improve security. Using hash code, attacker may find it difficult to identify password, however, it should not be ignored that, attacker can gain access to your account if you have weak password or poor login protocols.

Atharva Tendulkar
SE-CMPN-B





Password Managers

Now-a-days everyone has some online profile that they have secured with the use of credentials such as username, passwords, credit card credentials, aliases and. However, most security experts have come to recognize that passwords are inadequate by themselves. Users need some additional verification procedures to make their online profiles truly secure.

Problem with most insecure credentials is that they need to be remembered accurately and need to be changed every few months so that their profiles remain secure from social engineering attacks. It is also important for users to use different credentials on each different profiles, so that if one profile is breached other profiles remain secured. Users soon reach upto 50 password each very quickly and it becomes really difficult to remember these passwords. For a password to be secure following criteria need to be met:

- They must be changed every 60 days.
- They need to be at least eight characters long.
- They should use both upper and lower case characters.
- They must contain a combination of alphanumeric characters and symbols.
- They need to be unique (different password for different websites).
- Must be stored with a reversible encryption.

Enter the concept “Password Managers”. Password Managers are secure software(s) and services provided by various companies. These services store your credentials with a state-of-the-art encryption techniques and also allow you to use these passwords with just one click using auto-fill APIs. There are various password managers available today. Some of these services also allow you store other credentials such as credit card information and app-specific codes.

Password Managers are secure software(s) and services provided by various companies. These services store your credentials with a state-of-the-art encryption techniques and also allow you to use these passwords with just one click using auto-fill APIs.

While a user still needs to change these passwords every 60 days, password managers replace these on the next use. Also, password managers remind you to change these passwords too. They also provide you with a complex passwords that are and illegible to normal people which you can copy paste into the required fields. These passwords are generated mathematically. These password managers are also cross platform so that they can be used on any devices. They are available in the form of mobile apps, desktop apps, browser plugins, website and even system services.

LastPass is one of the most popular password managers on account of it being free completely. It provides a desktop app, a browser plugin for most popular browsers, a mobile app and a website as well.

Android Oreo 8.0 by Google makes use of the auto-fill APIs to simulate a password manager as a system service. Apple makes use of iCloud Keychain from IOS 7 to provide same functionality to iOS users.

It is prudent for the 21st century internet users to make use of these password managers to keep their credentials secured while also being easy to use. Password managers offer best of both worlds. Users also get to use complex encrypted passwords while they are also easier to use than normal username and password as they are one-click options.

***Chaitanya Chaphalkar
Rashi Dhariwal
Shivani Kulkarni
BE-CMPN-A***



Cyber Terrorism

Cyber or Cyberspace: the notional environment in which communication over computer networks occurs

Terrorism: even though elusive, it means the unlawful use of violence and intimidation, especially against civilians, in the pursuit of political aims.

Amalgamating the two definitions we get **"Cyber terrorism is the premeditated, politically motivated attack against information, computer systems, computer programs, and data which result in violence against noncombatant targets by sub national groups or clandestine agents."**

Cyber-terrorism is one of the major threats in today's world, and it's more likely to remain a threat for a long-long time in the future. This has taken the dangers, and the effect of terrorism to a whole new level.

Threats:

We live in an era of Information Technology, where 68% of adults are using digital phones, and almost 90% of people are using some kind of technology daily. Since our whole future seems to be based on technology, it makes 100% of us vulnerable to cyber attacks. Cyber contains all kinds of information, private, secret and could get into the hands of anyone now.

Ginni Rometty, IBM's chairman, president and CEO, said, "Cyber crime is the greatest threat to every company in the world."

Just imagine all the things you keep online, your emails, your photos, your documents, your files! These things can easily be stolen, or destroyed. Your whole system can be taken over by Ransomware. Cyber terrorists can endanger the security of the nation by targeting the sensitive and secret information

The effects of cyber terrorism can be:

- DDoSing a political party's website during an election
- Releasing hacked emails in an attempt to influence an election
- Attacking an industrial target as part of a larger terrorist campaign

In September last year details about India's top secret Scorpene submarine program were published online yet it failed to make the news. Up till June this year, 27,482 Cyber attacks have been reported. Which itself calls for an urgent need of Cyber-security.

The Problem:

Technology is updating so fast, that it might become very difficult to cope up with. The whole idea of DIGITAL INDIA can also make us even more vulnerable from the cyber attacks. Due to the lack of awareness most of us don't know how to defend ourselves from these attacks, or many of us fail to recognize the magnitude of threat we are in.

Cyber terrorism is much cheaper than the traditional terrorism, It is very difficult to be tracked. It can be done from anywhere in the world. This can affect a large number of people.

Need of cyber-security has to be acknowledged by the whole world. But to protect each and every system out there and to spread awareness to the whole world is practically very difficult.

We need better institutions in Cyber-Security

"Every computer system is theoretically penetrable." It is a fact that we must all accept, the problem is we can defend against those attacks that has already happen but hackers out there are finding newer ways to penetrate the systems. It is incomprehensible to defend against attacks we don't know about.

Solution:

Things we can do personally is, we can protect it with a password, unique and difficult of guess.

Keep the systems upgraded.

Audit systems.

Recognize suspicious email and website and report it.

Stages of defence would be:

- 1) Prevention
- 2) Incident Management
- 3) Consequence Management

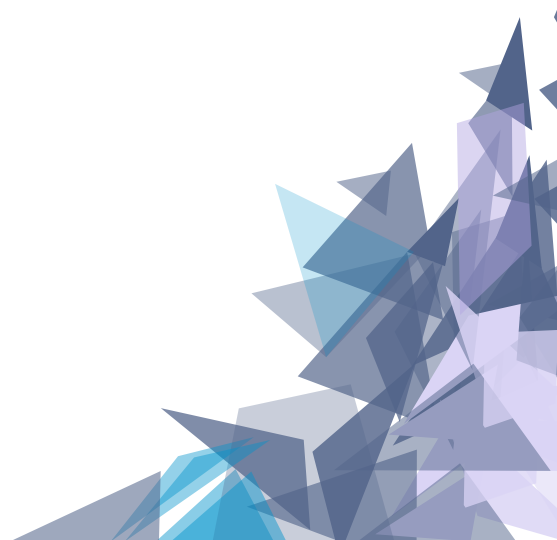
By being aware of these attacks, we can learn a lot of ways to defend against such threats. A lot of Research and Development has to be done in this area.

We need effective laws enacted by the legislature to defend against these malware and safeguard the public interest.

The whole world is trying to come up with the solution to Cyber-terrorism but it is impossible for them to do without the public support. We, people in general are taking this too lightly! In the fictional TV series 'Mr. Robot' exhibit the possibility and the extent of cyber attacks(In which the main protagonist aims to remove the debt by hacking into the central banks) Despite it being fictional, theoretically it is still possible for a hacker to find a vulnerability in a blockchain and disrupt the operability of it in some way.

Some hackers usually turn out to be computer geniuses and we need to find a way to identify them early and thwart them from the influence of terrorism. We need to be able to turn these cyber criminals into assets since that has worked quite successfully in the past. We must prepare our youths against the threat of cyber-terrorism.

Rohan Gupta
BE-CMPN-A



Cyber Terrorism Cases

Cyber terrorism is the use of the Internet to conduct violent acts that result in or threaten the loss of life or significant bodily harm in order to achieve political gains through intimidation. It is also sometimes considered the act of Internet terrorism in terrorist activities, including acts of deliberate, large-scale disruption of computer networks, especially of personal computers attached to the Internet, by the means of tools such as computer viruses. These crimes occur against individuals, businesses, organizations, and against the government itself.

Types of Cyberterror Capability:

The following three levels of cyber terror capability is defined by Monterey group-

1. Simple-Unstructured: The capability to conduct basic hacks against individual systems using tools created by someone else.
2. Advance-Structured: The organization possesses an elementary target analysis, command and control, and learning capability.
3. Complex-Coordinated: The capability for a coordinated attack capable of causing mass-disruption against integrated, heterogeneous defences (including cryptography).

Examples of Cyber Terrorism:

- Terrorism can occur over the public internet, over private computer servers, or even through secured government networks. There are many ways in which a criminal could use electronic means to incite fear and violence. It can be anonymous and conducted at a great distance away from the target.
- Foreign governments may use hackers to spy on U.S. intelligence communications in order to learn about where our troops are located or otherwise gain a tactical advantage at war.
- International terrorists could try to access and disable the signal which flies drones or otherwise controls military technology.
- Domestic terrorists may break into the private servers of a corporation in order to learn trade secrets, steal banking information, or perhaps the private data of their employees.

Current state of attack:

Every day the Internet and countless other computer systems are under attack. In the 2002 research study conducted by the Computer Crime Research Center, 90% of respondents detected computer security breaches within the last twelve months. In another more recent study, 92% of companies have experienced computer attacks and breaches in the last 12 months. If that is not shocking enough, security professionals are worried about the increased sophistication of threats against computer systems.

Here are some interesting statistics.

- Attacks against the Internet increase at an annual rate above 60%.
- The average business will experience 32 break-in attempts this week.
- Reported systems vulnerabilities and security incidents are doubling each year.
- 10% of security incidents and number of vulnerabilities were reported of total actual.
- There were more than 190,000 Internet based attacks on business, in the first half 2002.

Cases:

1. In 1996, a computer hacker allegedly associated with the White Supremacist movement temporarily disabled a Massachusetts ISP and damaged part of the ISP's record keeping system. They had attempted to stop the hacker from sending worldwide racist messages under the their name. The hacker backed off with the threat, "you have yet to see true electronic terrorism. This is a promise."

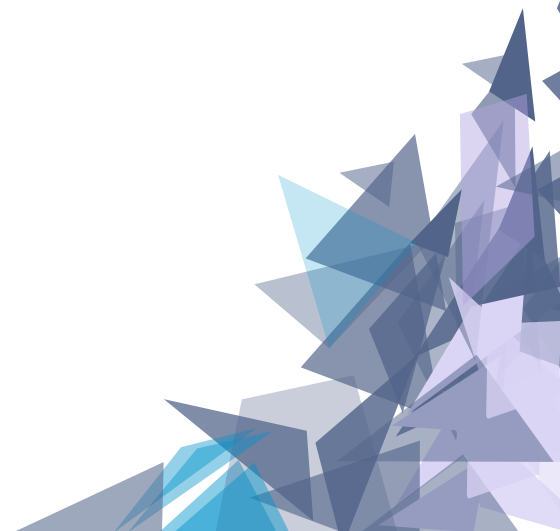
2. In 1998, ethnic Tamil guerrillas attempted to disrupt Sri Lankan embassies by sending large volumes of e-mail. The embassies received 800 e-mails a day over a two- week period. "We are the Internet Black Tigers and we're doing this to disrupt your communications." is what the email said. It was marked as the first known attack by terrorists on a country's computer systems.

3. July 2009-These were a series of attacks against government and news agencies of both the United States and South Korea. Overloading of servers was caused due to flooding of traffic by hacked computers. Total number of 263,000 were computers were hijacked and varied in its sources.

4. India- India has reported 13,301 cyber security breaches in 2011, despite its reputation for being an IT and software powerhouse. The biggest cyber-attack occurred on July 12, 2012 wherein hackers accessed the email accounts of 12,000 people.

5. Citigroup- Citigroup provides a great platform for hackers. In 2011, over 200,000 customer information from contact details to account numbers were compromised, which resulted in 2.7 million dollars loss for the company.

Harsheen Kaur
SE-CMPN-A



A zero-day vulnerability is an undisclosed computer-software vulnerability that hackers can exploit to adversely affect computer programs, data, additional computers or a network. Zero-day attacks are the attacks against system flaws that are unknown and have no patch or fix. With traditional defenses it is extremely difficult to detect zero-day attacks because traditional security approaches focus on malware signatures, this information is unknown in the case of zero-day attacks. It is known as a "zero-day" because it is not publicly reported or announced before becoming active, leaving the software's author with zero days in which to create patches or advise workarounds to mitigate its actions. Attackers are extraordinarily skilled, and their malware can go undetected on systems for months or even years which gives them plenty of time to cause irreparable harm . So, dealing with unknown vulnerabilities is clearly a challenging task. although there are many effective solutions like IDS/IPS, firewalls, antivirus, software upgrading and patching for tackling known attacks. Discovering unknown vulnerabilities and figuring out how to exploit them is clearly a challenging task.

Zero day attack exploits zero-day vulnerability without any signature. The anti-virus products cannot detect the attack through signature-based scanning and because the vulnerability is unknown, the affected software cannot be patched . These unpatched vulnerabilities are free pass for attackers to any target they want to attack . These zero-day attacks are most difficult to defend because after attack only the data get available for analysis.

During the past few years, the rapidly growing use of network services presents the biggest challenge in protecting computing environment for being everything digital. Every day the world of digital information security faces new challenges; an incredible flood of new devices is challenging tradition methods of securing organization's network. Therefore, the overall security level of a network cannot be measured by simply identifying the number of known vulnerabilities present in the system. The safer network configuration has little value if it is vulnerable to zero-day attacks. Zero-day attacks pose a serious threat to the organization's network, as they can exploit unknown vulnerabilities. The vulnerabilities that are unknown could cause harm at any level of the system's security because of unavailability of patches. Also, the security risk level of unknown vulnerabilities is difficult to measure due to less predictable nature.

TRADITIONAL DEFENSES AGAINST ZERO-DAY ATTACKS

Any organization connected to the internet has one common threat of zero-day attacks. The purposes of these attacks are, sensing confidential information, monitoring target's operations, theft of commercial information and system disruption. The primary goal of defense techniques is to identify the exploit as close as possible to the time of exploitation, to eliminate or minimize the damage caused by the attack. The research community has broadly classified the defense techniques against zero-day exploits as statistical-based, signature-based, behavior-based, and hybrid techniques

A. Statistical-based attack- Statistical-based attack detection techniques maintain the log of past exploits that are now known. With this historical log, attack profile is created to generate new parameters for new attacks detection. Statistical-based techniques build attack profiles from

historical data, which are static in nature; therefore they are not able to adopt the dynamic behavior of network environment. So, these techniques can't be used for detection of malware in real time.

B. Signature-based attack-For detection of polymorphic worms, signature-based techniques are used to identify their new representations on each new infection. These techniques are generally used by virus software vendors who will compile a library of different malware signatures. These libraries are constantly being updated for newly identified signatures of newly exploited vulnerabilities. Signature-based techniques are often used in virus software packages to defend against malicious payloads from malware to worms.

C. Behavior-based attack- These techniques rely on the ability to predict the flow of network traffic. Their goal is to predict the future behavior of network system in order to resist the anomalous behavior. The prediction of future behavior is done by machine learning approach through the current and past interactions with the web server, server or victim machine.

Protection

Zero-day protection is the ability to provide protection against zero-day exploits. Since zero-day attacks are generally unknown to the public, it is often difficult to defend against them. Zero-day attacks are often effective against "secure" networks and can remain undetected even after they are launched. Thus, users of so-called secure systems must also exercise common sense and practice safe computing habits

The Zeroday Emergency Response Team (ZERT) was a group of software engineers who worked to release non-vendor patches for zero-day exploits. The team included several members prominent in antivirus and network security work.

Their manifesto states: "ZERT members work together as a team to release a non-vendor patch when a so-called "Oday" (zero-day) exploit appears in the open which poses a serious risk to the public, to the infrastructure of the Internet or both. The purpose of ZERT is not to "crack" products, but rather to "uncrack" them by averting security vulnerabilities in them before they can be widely exploited."

Vulnerabilities appear in almost every organization, but the most attractive to targeted attackers is software that is widely used. Most of the vulnerabilities are discovered in software such as Internet Explorer and Adobe Flash, which are used frequently by a large number of consumers and professionals. After discovery, the zero-day attacks are quickly added to attackers' toolkits and exploited. Networks are dynamic in behavior with uncertainties, so new method should regularly be sought to prevent malicious attackers from exploiting unknown vulnerabilities. The anomaly detection technique is used to discover anomalies and thus to identify the zero-day attack types using an assigned anomaly score. The proposed method is effective and efficient in detecting zeroday attacks than the typical statistical based anomaly detection techniques.

Shrutika Agarwal
SE-CMPN-A



The Latest Global Cyber Attack: Ransomware



A highly vicious type of malware is ransomware, which is deceptively installed on your PC and locks the system down. That lockdown is inevitably accompanied by a message demanding payment if the PC's owner ever wants to access his or her files again. Unless you are very lucky, everything pith on your hard drive will be totally lost to you, unless you pay for it.

Although previous versions of ransomware sometimes had flawed encryption, recent changes are superiorly designed. Though you could pay the ransom, that's not an assurance that things will be solved, as Kansas Hospital in U.S discovered when hackers demanded a second ransom after locking down files. I recently had an irksome encounter with ransomware. Here's what actually happened:

The Case

The victim: a small taxi firm in West London with 10 networked PCs (five in a central office, with another five in small satellite offices located near the railway or London Underground stations). The system could take customer bookings via a custom-written Booking and Dispatch software. I'd performed some programming work for this company on an independent PC at their central office. One of the senior managers asked if I'd take a look at their main dispatch-server software. It wouldn't start after a reboot, it seemed. I had a background in writing cellular software that communicates with server software, so I knew enough to troubleshoot and check the issues. The server software ran on a desktop PC, with network shares to the other computers; a MySQL database held all the data. The software automatically delivered jobs to drivers, allowing a PC's operator to change or rebook jobs. In addition to failing to start, the system indicated a missing text file. All the company's computers ran Windows XP, except for two on Windows 7. Employees answered email using two of those PCs. After it became lucid that we had a malware problem, our best guess was that it had pierced the network through an email attachment.

The Malware

I identified the guilty party as Cerber ransomware, specifically a jejune variant that resisted efforts by utility programs such as SpyRemover to eliminate it. I also went through the registry settings as told by MalwareBytes, hoping to isolate the real nature of the problem, but had no luck. Cerber has a bad habit of deleting key files in its wake in order to astonish attempts to stop it. The company planned to restart the software and see how things went. While the server was down, though, the firm had to jot down new taxi orders on little chits of paper. It was total disarray. Each infected folder contained three files: My Files.html, .vbs and .txt. The ransomware encrypted any documents on the target extension list, giving it a totally random filename with the .cerber extension. The malware infected three PCs at the central office and two at satellite office companies; the other five weren't touched. The damage to these corrupted computers was remarkably low: the log files (.log) were all encrypted, as well as one config file (.txt) that the main server used for mapping West London into booking zones. After changing that file, the server was able to run it. The only major loss was the log files.

The Threat

The #Decrypt My Files.html had a message asking for 1.3 Bitcoins (about \$5391) to recover the computer, including main details on how to pay. No ransom was paid. The Taxi firm's M.D already had a secret plan to replace all computers in a few months, as most were seven to nine years old. That plan was accelerated, and all 10 PCs were changed one week after the initial malware. I returned a week after to help replace the computers and to my surprise discovered that no further corruptions had occurred since the first one. It's my belief that the malware just ran once from one computer and managed to infect four others. But this wasn't permanent, and it didn't reload after a reboot, so the malware was eliminated. A recent article in Magazine seemed to confirm that a different version of Cerber only exists in RAM. Meanwhile, another different article suggested that Cerber variants use PowerShell to alter their signature, but I can't be sure of that, as the taxi firm's PCs did not have

PowerShell installed on it.

Protection

Big companies always have dangerous plans in places that have ransomware viruses. But what should individuals or minute businesses do when confronted with this problem? Crossing your fingers is definitely not the best option possible. Recurrent offsite backups are the obvious initial step, though the automation comes with a downside: if your files are viciously encrypted, the encrypted files may accidentally get backed up, as well. If you take this route, always make sure that the backup vendor offers a 31-day recovery period, so you can get your backed-up files intact and ready. For individuals, even something as easy as copying files to an external memory drive is better than nothing. If you take this step, keep your USB storage unplugged from your PCs when not copying to it. As email attachments are a major source of infections, having an email scanner is probably the best possible way to eliminate that particular vector of threat.

I've been imagining about using email and Web-browsing only from within VirtualBox, which might keep any ransomware virus that evade detection from doing much problem. But if you don't want to consider paying a ransom, then the best solution for malware is complete preparation: back up your files in the initial stages. And if you are involved in a business, take the time to edify staff about the dangers and threats of opening email attachments, even if they know the actual sender.

Abhijeet Prasad
BE-CMPN-B



Top Ransomware Attacks



The Government of India introduced its flagship programme “Digital India” in July 2015. This programme was introduced to transform India into a digitally empowered Economy and so that government services were made available to the citizens electronically through digital media. Now in this era of digital evolution, all our information is to be stored digitally. The more digitally empowered we become, the more we are vulnerable to digital information threats and hacking. In this era where we set the most complicated pattern locks on our phones, imagine how much havoc can hacking cause to person and to what lengths a person may go to get all his data back.

There are so many new ways to hack into a system and get control of all kinds of important information. Some types of cyber attacks are as follows:

- **Malware-** These are types of viruses or ransomwares that enter the computer when an user clicks a screen pop up or opens an email or attachment. This malware can cause havoc on the system by either shutting it down, getting all the important information to the attacker or simply mess with system. Ransomware causes blocking of all access to a system, the attacker demands ransom to give back the user the systems access.
- **Phishing-** Phishing is the use of lucrative emails and attachments which the user just cannot resist or emails of urgency from someone the user trusts. When such emails are opened, the malware gets an entry in the computer system.
- **Denial of Service attack-** IN this type of DoS attack, the attacker or multiple attackers flood an website with multiple requests which causes traffic unmanageable by the website causing it to shut down or deny access.

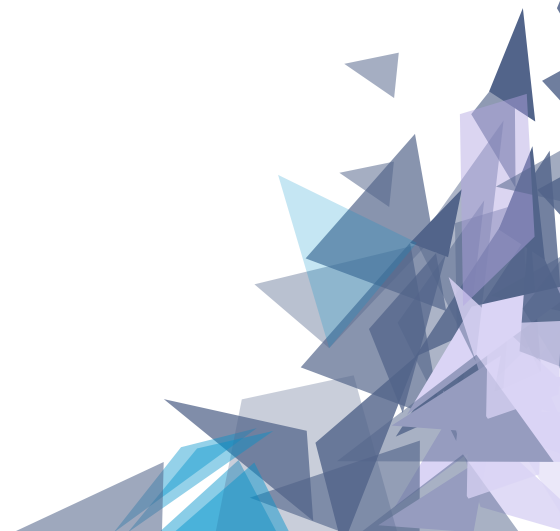
Everyone wants their data secure and one can do anything to protect access of their data. Imagine the scenario when a person has to pay to use his own data .People are ready to pay whatever the ransomwares asks for. Ransomwares have caused too much of commotion in the past few years and now, even the most secure companies have acknowledged the threat of an ransomware attack . Lets look at some of the major ransomware attacks in the recent years which have made the world fear for its information security:

1. Wannacry: Wanna Decryptor or simply wannacry is the biggest ransomware attack the world has witnessed. It started by the detection of a flaw in Microsoft's software. Microsoft did provide the solution of the flaw to the users, but many people were unaware of it.Wannacry used this to its advantage. It started in Europe and rapidly managed to attack over 116 countries all over the world .At least 250,000 detections of wannacry attack were found. Once the system is attacked, the attacker blocks access to the system and provides the victim with two files. One file provides instructions on what to do next and the payment. The second file is the Wannacry software itself. The payment method is bitcoins ,the latest type of cryptocurrency ,as it is impossible to trace.

2. NotPetya: Petya was a ransomware launched in 2016 which mainly targeted Windows-Microsoft systems. They blocked access unless payment was made in Bitcoin.in 2017,this ransomware was back but it had difference in operation. NotPetya, unlike former Petya was most likely developed to cause havoc and destroy all information from the victims' systems. The attack as speculated and debated, was launched to attack all information of the attacked system in Ukraine. This quickly spread to Russia, US and parts of Asia, Europe and Australia. NotPetya demands all its victims to pay to a single bitcoin address and asked them to email a long string of characters typed manually to an email address which doesn't even work. This attack wasn't a ransomware at all as the hackers just wanted to cause damage and commotion and keep the fame of WannaCry ransomware alive.

The only precautions to not getting attacked by a ransomware is to keep a back up of our data separately. Never click on unsecure links or open random emails or click onto pop up alerts. Use a good anti-virus and anti-ransomware. Never keep passwords unchanged for too long or reuse passwords for multiple accounts or use easy characters like name or birthdays as passwords. Never share our account details and always keep your accounts private.

Nirja Rajeev
SE-CMPN-B





Cryptocurrencies



Cryptocurrency is a digital currency in which encryption techniques are used to regulate the generation of units of currency and verify the transfer of funds, operating independently of the bank. Few people know, but cryptocurrencies emerged as a side product of another invention. Satoshi Nakamoto, the inventor of Bitcoin, never intended to invent a currency. Bitcoin is the first and still most important cryptocurrency. In his announcement of Bitcoin in the late 2008, Satoshi said he developed “A Peer-to-Peer Electronic Cash System”. His goal was to invent a system to digitally transfer assets. Announcing the first release of Bitcoin, a new electronic cash system that uses a peer-to-peer network to prevent double-spending. It’s completely decentralized with no server or central authority. – Satoshi Nakamoto, January 2009, announcing Bitcoin. The single most important part of Satoshi’s invention was that he found a way to build a decentralized digital cash system. In the 90s, there have been many attempts to create digital money, but none of them worked successfully. After seeing all the centralized attempts fail, Satoshi tried to build a digital cash system without a central entity, like a Peer-to-Peer network for file sharing. This decision became the birth of cryptocurrency.

Mechanism:

To accomplish digital cash we need a payment network with accounts, balances, and transaction. One major problem every payment network has to solve is to prevent double spending: to prevent that one entity spends the same amount twice. Usually, this is done by a central server who records about the balances. In a decentralized network, you don’t have this server. So you need every single entity of the network to do this job. Every peer in the network needs to have a list of all transactions, to check if future transactions are valid and are not an attempt to double spend. If the peers of the network disagree about only minor balance, everything is broken. They need an absolute agreement. Usually, you take, again, a central authority to declare the correct state of balances. But how can you achieve agreement without a central authority? Cryptocurrencies is the solution.

The Malware:

I identified the guilty party as Cerber ransomware, specifically a jejune variant that resisted efforts by utility programs such as Spy Remover to eliminate it. I also went through the registry settings as told by Malware Bytes, hoping to isolate the real nature of the problem, but had no luck. Cerber has a bad habit of deleting key files in its wake in order to astonish attempts to stop it. The company planned to restart the software and see how things went. While the server was down, though, the firm had to jot down new taxi orders on little chits of paper. It was total disarray. Each infected folder contained three files: My Files.html, .vbs and .txt. The ransomware encrypted any documents on the target extension list, giving it a totally random filename with the .cerber extension. The malware infected three PCs at the central office and two at satellite office companies; the other five weren't touched. The damage to these corrupted computers was remarkably low: the log files (.log) were all encrypted, as well as one config file (.txt) that the main server used for mapping West London into booking zones. After changing that file, the server was able to run it. The only major loss was the log files.

The Threat:

The #Decrypt My Files.html had a message asking for 1.3 Bitcoins (about \$5391) to recover the computer, including main details on how to pay. No ransom was paid. The Taxi firm's M.D already had a secret plan to replace all computers in a few months, as most were seven to nine years old. That plan was accelerated, and all 10 PCs were changed one week after the initial malware. I returned a week after to help replace the computers and to my surprise discovered that no further corruptions had occurred since the first one. It's my belief that the malware just ran once from one computer and managed to infect four others. But this wasn't permanent, and it didn't reload after a reboot, so the malware was eliminated. A recent article in Magazine seemed to confirm that a different version of Cerber only exists in RAM. Meanwhile, another different article suggested that Cerber variants use PowerShell to alter their signature, but I can't be sure of that, as the taxi firm's PCs did not have PowerShell installed on it.

Protection:

Big companies always have dangerous plans in places that have ransomware viruses. But what should individuals or minute businesses do when confronted with this problem? Crossing your fingers is definitely not the best option possible. Recurrent offsite backups are the obvious initial step, though the automation comes with a downside: if your files are viciously encrypted, the encrypted files may accidentally get backed up, as well. If you take this route, always make sure that the backup vendor offers a 31-day recovery period, so you can get your backed-up files intact and ready. For individuals, even something as easy as copying files to an external memory drive is better than nothing. If you take this step, keep your USB storage unplugged from your PCs when not copying to it. As email attachments are a major source of infections, having an email scanner is probably the best possible way to eliminate that particular vector of threat.

I've been imagining about using email and Web-browsing only from within VirtualBox, which might keep any ransomware virus that evade detection from doing much problem. But if you don't want to consider paying a ransom, then the best solution for malware is complete preparation: back up your files in the initial stages. And if you are involved in a business, take the time to edify staff about the dangers and threats of opening email attachments, even if they know the actual sender.

Deep Suchak
BE-CMPN-B



Bitcoin

"A Peer-to-Peer Network"

What is Bitcoin?

- Software based online payment system described by Satoshi Nakamoto in 2008/Operational since early 2009.
- First decentralized digital/virtual Currency.
- Bitcoin is an International Currency.
- It is an Open source Project whereas bitcoin community have a core group of 30 members.
- Bitcoin is the Application of Blockchain.
- Blockchain is the Distributed Ledger.
- Bitcoin is only stored in Blockchain, Wallets do not store bitcoin.
- Biggest challenge of Bitcoin is to identify dual Spending.

Component of Bitcoin:

- Wallets
- Network
- Transaction
- Miners

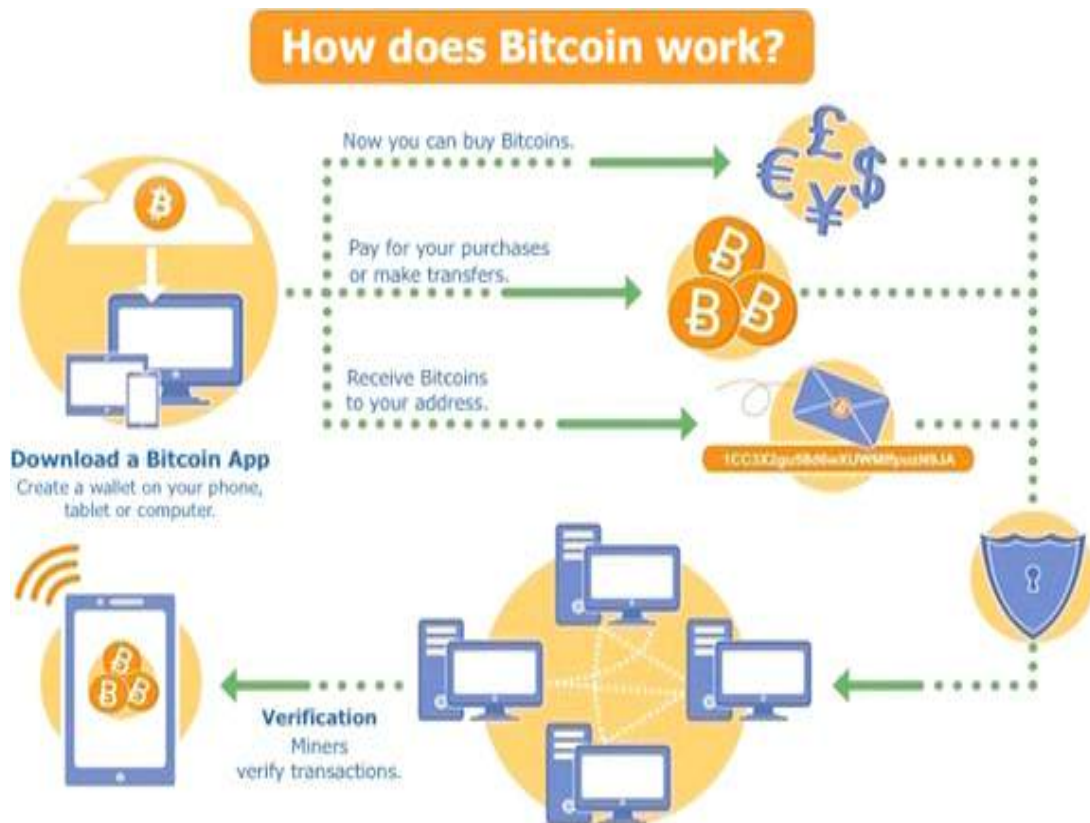
Features:

- Decentralized
- It is anonymous
- Completely Transparent
- Transaction Fee is minuscule
- Transaction are irreversible
- Fast and easy to setup

Environments in Bitcoin: 1) Mainnet 2) Testnet 3) Regtest

Who are miners?

Miners are primary converters of energy into Bitcoin.



Note:
After 60 minutes user can confirm that transaction is genuine and not dual transaction.
6 nodes must verify then the user is confirmed that transaction is genuine.

"...we don't really understand how that worked, as economists."

- Lawrence White, Economics professor at George Mason University / IEEE Spectrum interview.

Advantages:

- Freedom in payment
- Control and security
- Information is transparent
- Very low fees

Amit Tiwari
TE-CMPN-B

Disadvantages:

- Lack of awareness and Understanding
- Risk and Volatility
- Still Developing

Conclusion:

- BTC: P2P digital currency with mathematic protection
- No centralized control / No evil Central Bank



BLOCK CHAIN

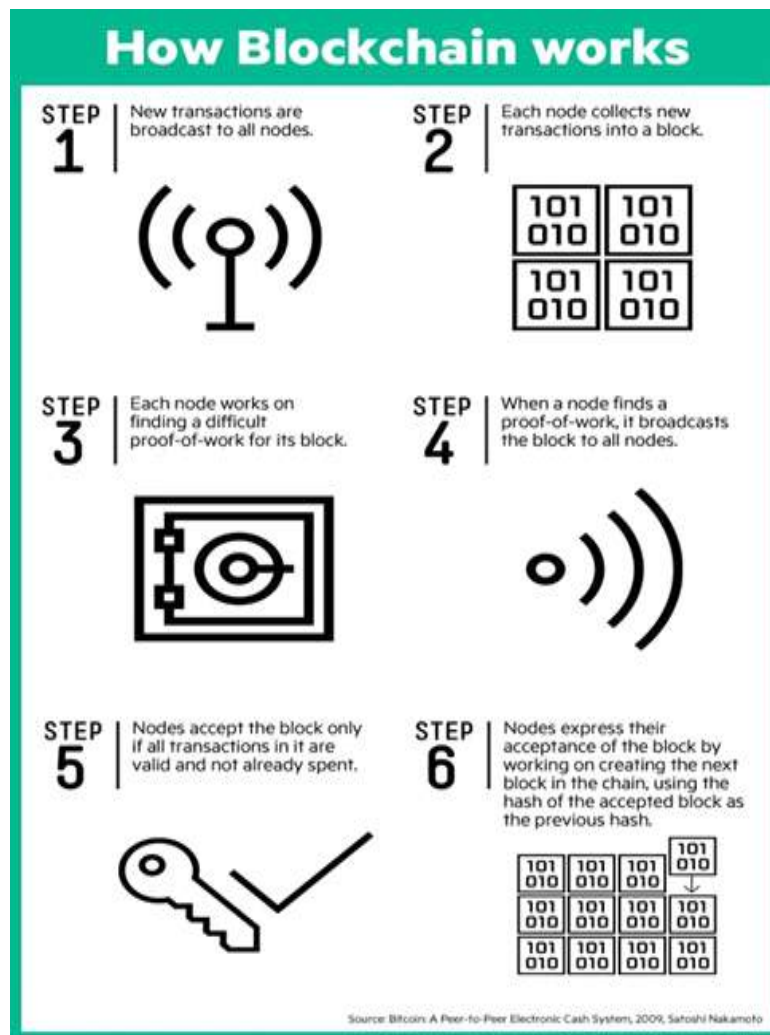
Block chain technology is a decentralized database that securely deals with transactions/data recorded about the assets (financial assets like bit coin, abstract assets like customer data).It is basically a publicly registry who owns what and who transacts what. The transactions are secured through cryptography and over a time, that transaction history gets locked in the block of data that then cryptographically linked together and secured. This creates an immutable unforgettable record of all transaction in network. It uses merkel tree.

Working:

Suppose, someone requests a transaction .The requested transaction is broadcast to a P2P networks consisting of computer known as nodes. The network of nodes starts validating the transaction and user's status using known algorithms. A transaction can be verified by performing a quick hash function that checks and instantly allows agree/confirm or disagree/reject of transaction due to this the problem of double spending are avoided . After verifying, the transaction is combined with the other transactions, so a new block of data for the ledger is created. Each time a new block is created it is added to the existing block chain which contains all the transactions from the genesis block (i.e first block) till the new transaction which is added.


Applications of block chain:

Aside from cryptocurrencies, there are a wide number of industries and services which have employed. It has being utilized by the financial and banking sector, governments (to store the database of the people etc.), health care industry to maintain the patient history, information security, smart contracts , internet of things and many more.



Block chain is link list using hash pointer which allow to detect any tamper of data. It is robust as it has transformative characteristics that provide high security of data. Since, it is builds on cryptography so the hackers can't manipulate the transaction /data in the block. As block chain is immutability nobody can change the transactions as data is recorded permanently. It provides anonymity; nobody has the details about your transactions.

Shriya Sundriyal
TE-CMPN-B



Are we at the verge of a security apocalypse by Artificial Intelligence?

"If I were to guess what our biggest existential threat is, it's probably that. So we need to be very careful with the artificial intelligence. With artificial intelligence we are summoning the demon."-Elon Musk

With quotes like this made by leading pioneer in this boom of intelligence in security , it is important for us to identify our position in AI and know what the future would hold in space for us.

Artificial intelligence (AI) has become such a buzzword , what people perceive to be AI is nothing more than a driving program of learning ,it has become such a pixie dust that namedropping is all it takes for simple body of if-else or decisive, controlled learning to be termed as the next big thing in AI .,just sprinkle a little here and suddenly, your solution inherits the foresight of a self-driving Tesla and the simplicity of an Amazon Echo,what even technology enthusiast like Stephen Hawking or Bill Gates don't understand is the vast difference between AI and ML,AI is a system that is conscious of it's surroundings, a sytem which can "think" , perceive without a stimulus, but are we even close to building a coherent system like this? The answer is clearly a No , this is illustrated by the following few quotes made by industry expert, those have extensively researched on this topic:

"I think people see how well [an algorithm] performs at one task and they think it can do all the things around that, and it can't," -Rodney Brook, MIT Professor

"I think it's important to keep in context how good these systems are, and actually how bad they are too, and how long we have to go until these systems actually pose that kind of a threat [that Elon Musk and others talk about]" -Gil Pratt, CEO, Toyota Institute..

What we are using right now in security is Machine Learning, which is a system that accepts a controlled input, processes it based on it's perceived understanding and gives an output. Should we use Machine Learning or AI for cyber security?

The answer is machine learning. .

AI implies cognitive introspection on the part of the tech -- an ability to improve itself based on understanding its own performance. We're nowhere near this yet.

ML is a subfield of computer science that helps computers learn based on their inputs and decide how to behave without being explicitly programmed to do so. The ML practitioner will approach the task with a large and developing toolset. Different algorithms have different uses, and techniques overlap with computational statistics, mathematical optimization and data mining.

An ML algorithm builds a model that represents the behavior of a real-world system from data that represents samples of its behavior. Training can be supervised - with pre-labeled example data -- or unsupervised. Either way, the data needs to be a representative of the real world. Without representative data, no algorithm can offer useful and generalizable insights.

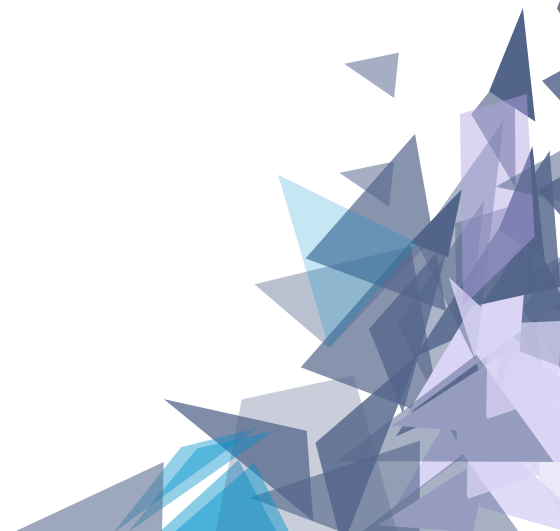
The challenge in cyber security is that the initial phases of an attack, such as Malware or spear-phishing emails, vary every time the attack is launched, making it impossible to detect and classify with confidence. With good training data, state-of-the-art ML algorithms can do a pretty good job of training a model that can then be used to sift through new, unlabeled data. The problem is the term "pretty good job." It's hard to know beforehand just how accurate the classification of new data will be. (Was the training data adequate? Is the model good at teasing apart the grey -- things that may be good, bad, etc.?) What's beyond doubt, however, is every algorithm will make mistakes. It could generate false alerts or fail to detect the bad guy.

As it is observed that ML performs really bad in irregular environments, it is only good for "crunching through data" ,it may be difficult to understand different points of data sets ML has provided has output as it is abstract in it's working. So, rather than trying to detect Malware before it executes -- as many "next-gen" vendors claim,

which by Turing's proof is a fool's errand -- when malware actually executes on an endpoint, it's easy to spot as a deviation from known normal behavior of the application it has attacked.

To overcome these drawback of primitive ML there has been a lot of research currently going on in cognitive ML, which if implemented correctly comes close to an Intelligent system, one that can think through it's 5 senses, this type of system can sense a malware extensively in a system and deactivate it before any damage, the professors at MIT's Robotics Lab believe that AI can be fully developed withing the next 100 years and though there are less chances of this technology to be used for the worse , they have signed up for a robust system by the FLL (Future Of Life Letter).

Vani Singala
BE-CMPN-B





Career Opportunities in Cyber Security

Launch your career in a high demand industry that projects 2 million new jobs annually!

Job Outlook

- Exciting career opportunities as security analyst, security engineer, security architect, forensics investigator, cybersecurity specialist, and more!
- Cybersecurity positions are expected to rise 6 million globally by 2019 (source: Forbes, January 2016)
- If you are already in the IT field, expect a 9% raise in pay for security expertise (source: Forbes, January 2016)
- Median salary for information security analyst for 2015 is \$90,000 (source: US Bureau of Labor Statistics)

Real Career Impact

The shortage of skilled and qualified cybersecurity professionals is one of the biggest issues facing our Internet-connected world today. This gap can be closed. Professionals who gain the skills and tactics needed to defend against the next generation of security threats will be better prepared for careers at various organizations in the cybersecurity industry.

What you need to learn:

- How to setup and secure basic computer systems and networks.
- Information security risk management framework and methodologies.
- How to implement network security solutions and detect intrusions.
- How to conduct a digital forensics investigation admissible to a court.
- To practice cybersecurity skills in real world scenarios.

Career path options

There is no one true path to working in cyber security. People come at it from all angles – math, computer science, even history or philosophy. Yet all of them share a deep and abiding interest in how technology works. Security gurus say this is critical. You need to know exactly what you're protecting and the reason things are insecure.

Focus on your interests

Because it's impossible to be an expert in all categories, employers also suggest you focus on an area (e.g. networking security) and do it well. Think ahead 5-10 years to your "ultimate security career" then look for starter jobs that will supply you with the right skills. Sample career paths could include:

- Exchange administrator → Email security
- Network administrator → Network security, forensics, etc.
- System administrator → Security administrator, forensics, etc.
- Web developer → Web security, security software developer, etc.

How to be an Ideal Candidate?

The ideal cyber security candidate has a mixture of technical and soft skills. On the technical side, most employers want proof that you are:

- Grounded in fundamentals: e.g. networking, systems administration, database management, web applications, etc.
- Versed in day-to-day operations: e.g. physical security, networks, server equipment, enterprise storage, users, applications, etc.

For soft skills, they're looking for candidates who:

- Know how to communicate with non-IT colleagues and work in a team.
- Understand business procedures & processes.
- Love to solve complex puzzles and unpick problems.

Self-directed Learning

- Teach yourself to code. (Experts recommend this again and again.)
- Build your own computer and security lab using old PCs, your own wireless router with firewall, network switch, etc. Practice securing the computer and network, then try hacking it.
- Create an open source project.
- Participate in cyber security contests and training games. e.g. Wargames, Capture the Flag competitions (CTFs), etc.
- Look for vulnerabilities on open source projects and sites with bug bounties. Document your work and findings.

Guided Training

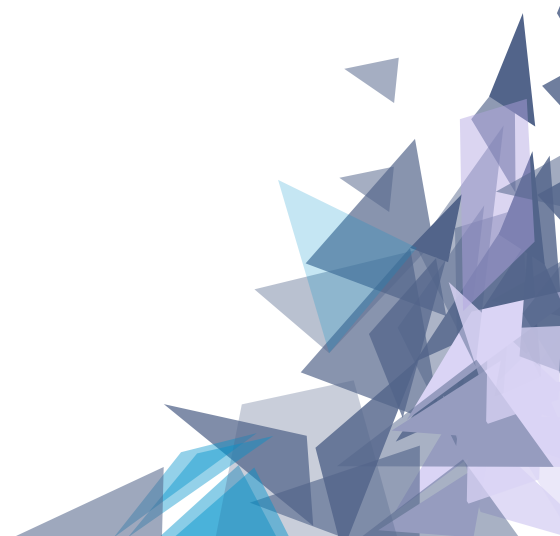
- Pair your cyber security certification exams with side projects that utilize the same skills.
- Offer to help your professor or employer with security-related tasks.
- Take free online cyber security Massive Open Online Courses (MOOCs)
- Invest in training courses (e.g. SANS).

Future Steps

- Read IT and security magazines/news sites and blogs.
- Bookmark useful cyber security websites.
- Keep tabs on cyber security message boards like Information Security Stack Exchange.
- Run a background check on yourself to see if there are any existing red flags, then determine what you can do to address them. Security is a sensitive field and employers are looking for ethical candidates.

All the best!

Akshay Hegiste
Software Tester, Amazon





SHUBHAM VISHWAKARMA	10.0
SHAHEEN	10.0
SIMRAN MALAWAT	9.92
VAIDITYA CHAUHAN	9.83
PRINCE SINHA	9.83

SHREYA HEGISTE
ANKIT GUPTA
HIRESH JOSHI
VIPUL AGARWAL
MEHER DODHIA

9.68
9.54
9.50
9.21
9.14



PRASHANT KAPRI	9.76
AISHWARYA GUPTA	9.44
SMRITI SINGH	9.33
ROHIT SINGH	9.30
SHUBHAM YADAV	9.15
SANDESH GADE	9.15



AMIT TIWARI

*Semi- Finalist at Code Galdiators
IBM Hackathon,
Secured 519 Rank in Cloud
Computing*

SAURABH SINGH
ANAND SINGH
DIVIJ SHAH
ADITYA RAI

*Internship in IONIC
Mumbai 28 Tech*



PRASAD POL

*Microsoft Certification in
Software Development and
Database Fundamentals*





GAUTAM SHARMA

Certification course by Coursera
on Machine Learning, Linear
Algebra edX

RAVISHANKAR SINGH

CEH v9 (Certified Ethical
Hacking) by ECCouncil



AYNSH AGARWAL

2nd Price Winner in Chess
Competition
conducted by Mumbai University



ANSHUL GUPTA
VARUN MALVIA
HITESH JHA
PRITESH BANSAL

Internship in Iterative Solution

SHREYA SINGH
AKSHARA SETHI
SWATIK CHAVAN
VEDASHREE DALVI
SALONEE AMERICA
MAHIMA JAIN
SHRUTIKA AGRAWAL
RUTAM LAVANAR

*CSI Poster Competition
Winners*



GAUTAM SHARMA

Finalist at the IIT Bombay E-
Yantra Robotics
Competition, Finalist at Cisco
India's Biggest Networking
Championship (IBNC)





PRAKASH SHUKLA

Worked as an Active Member of A national level NGO 'Action for Collective Transformation' (ACT).

SHUBHAM CHHAPARIA

*Internship at "Grapevine Co."
and "HITGodrej"*



Student Editorial Committee



*(L-R): Tejas Gupta, Sagar Pathare, Mrinal Bageshwari,
Adit Rathi, Athashree Vartak & Saurabh Jha*

Acknowledgements

Success is the result of perfection, hard work and determination. Team Nimbus has always been dedicated in bringing the best Nimbus every semester. With the same determination, we have worked hard to bring this edition.

We would like to extend our deepest gratitude to the Chairman, Trustees and CEOs of Thakur Educational group. Also, we are deeply thankful to our Principal, Dr. B.K. Mishra and Mentor Dean, Dr. R.R. Sedamkar for their constant encouragement and support.

Heartiest accolades for our HOD Dr. Sheetal Rathi and Faculty In-charge Mrs. Harshala Yadav, without them Nimbus wouldn't have been what is today.

At the end we would like to express our sincere thanks to all the students, teachers and industry experts for providing us with their valuable inputs through articles and interviews.

-Team Nimbus 6.0