Issue 2

<Inspire>

Newsletter

Department of Information Science & Engineering

Volume 3

June - 2018

Vision and Mission of the Institute

Vision

- To be one of the premier Institutes of Engineering and Management education in the country.

Mission

- To provide Engineering and Management education that meets the needs of human resources in the country.
- To develop leadership qualities, team spirit and concern for environment in students.

Objectives

- To achieve educational goals as stated in the vision through the mission statements which depicts the distinctive characteristics of the Institution.
- To make teaching-learning process an enjoyable pursuit for the students and teachers

Vision and Mission of the Department

Vision

- To be a premier department of learning in Information Science and Engineering in the state of Karnataka, moulding students into professional Engineers.

Mission

- Provide teaching-learning process that develops core competencies in Information Science and Engineering to meet the needs of the industry and higher education.
- Create an environment for innovative thinking and self-learning to address the challenges of changing technology.
- Provide an environment to build team spirit and leadership qualities to succeed in professional career.
- Empathize with the societal needs and environmental concerns in Information Science and Engineering practices.

Eugene Kaspersky

Eugene Kaspersky (born 4 October 1965) is a Russian cybersecurity expert and the CEO of Kaspersky Lab, an IT security company with 4000 employees. He cofounded Kaspersky Lab in 1997 and helped identify instances of government sponsored cyberwarfare as the head of research. He has been an advocate for an international treaty prohibiting cyberwarfare. His interest in IT security began when his work computer was infected with the Cascade virus in 1989 and he developed a program to remove it. Kaspersky helped grow Kaspersky Lab through security research and salesmanship. He became the CEO in 2007 and remains so as of 2018.

Kaspersky is influential among security experts. Kaspersky was ranked #1,567 on Forbes' "Billionaires List 2017". We dedicate the current issue of INSPIRE to Kaspersky.

Contents

B. N. M. Institute of Technology

Vidyaya Amrutham Ashnuthe

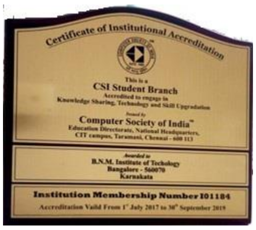
Approved by AICTE, Affiliated to VTU, ISO 9001:2008 Certified and Accredited as grade A Institution by NAAC
Post box No. 7087, 27th Cross, 12th Main, Banashankari II Stage, Bengaluru- 560070, INDIA
Ph: 91-80- 26711780/81/82 Email: principal@bnmit.in, bnmitprincipal@gmail.com, www.bnmit.org

Message from the Editorial Team

Greetings from the editorial team! Social media and emerging mobile technologies have changed the landscape of human interaction. Understanding the importance of this rapid technology shift, we present to you the current issue of the newsletter with the theme “Data Security”. Hope this edition would be as enlightening to you as it was for us. Happy apprehending!

About The Department

The department of Information Science & Engineering was established in the year 2001 and has forged a path of academic excellence and innovative teaching. The department has a diverse community of faculty involved in various research activities, teaching and mentoring students. Students are encouraged to participate in technical events and to conceptualize innovative ideas. The department is associated with many professional societies like IEEE, CSI, BITES etc. The Information Science & Engineering Association (ISEA) regularly organizes technical events for the benefit of the students.



Certificate of Institutional Accreditation

This is a

CSI Student Branch

Accredited to engage in

Knowledge Sharing, Technology and Skill Upgradation

Issued by

Computer Society of India™

Education Directorate, National Headquarters,
CIT campus, Taramani, Chennai - 600 113

Awarded to

B.N.M. Institute of Techology
Bangalore - 560070
Karnataka

Institution Membership Number I01184

Accreditation Valid From 1st July 2017 to 30th September 2019

BNMIT – CSI Student branch received certificate of institutional accreditation by Computer Society of India, Chennai for the period 1st July 2017 to 30th September, 2019. It is accredited to engage in knowledge sharing, technology and skill upgradation

Workshop and Technical Talks

Students from the department of ISE visited IoT Exhibition in KTPO Trade center Whitefield on 9th Feb 2018 conducted as part of the Indian Electronic Week 2018. 148+ companies showcased their innovations at the exhibition. Most of the innovations were related to AI and Home Automation. Some important companies that were present in the event were 3C TAEYANC, CHIPMAX Design PVT limited and EMSOL Systems. Students had the opportunity to interact with different companies.

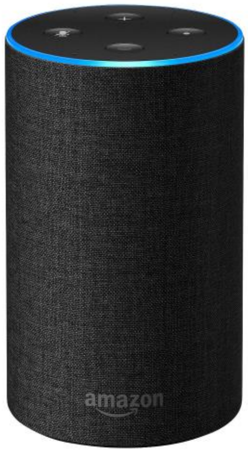
BNM Institute of Technology in association with BITES organized a workshop on “Professional /Managerial Communication” for students of 4th and 6th semesters of all branches of BNMIT on 9th -10th & 23rd -24th Feb 2018. Resource person for the workshop was Mr. Rakesh Gowdhwani, Adjunct Faculty, IIM Bangalore. The objective of the workshop was to outline the principles and role of communication in strengthening interaction and hence building confidence in students.

A workshop on Virtual Reality was conducted in collaboration with ITC-IIT, Mumbai under CSI-BNMIT student branch on 16th and 17th March, 2018. The resource person, Mr. Janardhan Chaudhary is a design engineer at Design Technology. The topics covered with hands-on session were: Need of Virtual Reality, comparison between different VR headsets, Google cardboard, Unity software tool, importing Google VR SDK to Unity, Linking Unity with Android Studio. Students have developed Maze game as an outcome of the workshop. Technical test and evaluation of the game was conducted at the end of the workshop.

The average cost of a data breach will exceed $150 million as more business infrastructure gets connected

Amazon's Alexa Hacked to Surreptitiously Record Everything It Hears

Voice-activated assistants like Amazon's Alexa and the Google Assistant are convenient and powerful tools for getting information and carrying out tasks. They also raise privacy questions because they record their interactions with the user and are always-on waiting to hear their wake-up command. What the voice-activated assistants hear, and record is limited in normal use, but the potential for abuse is a cause for concern. That potential has now been realized. Alexa has been hacked to surreptitiously record everything it can hear.



Checkmarx makes a suite of tools for developers to test the security of their software before it's released to the public. The researchers at Checkmarx have demonstrated how Alexa can be hacked to record what it hears. When Alexa operates as intended, it wakes up when it hears "Alexa", follows a limited script for the app that is activated, records the user's interaction with the script, and shuts down after Alexa executes the requested response. A hacker needs to break into and modify this tightly controlled sequence to subvert Alexa for malicious purposes. Checkmarx attached their malicious code to a seemingly innocuous app. The company used a simple calculator app for demonstration purposes. Getting Alexa to continue recording after the benign script in the app was executed proved more difficult. Checkmarx had two problems to solve. Alexa needed to keep listening after the benign response was given without alerting the user, and it had to record what it heard.

Checkmarx took advantage of two Alexa functions to surreptitiously prevent the system from shutting down after the benign response was given. Alexa has a flag that allows a session to remain open if an app needs a second response from the user. For example, if you tell Alexa to set an alarm for 7:30, Alexa will ask if you mean 7:30 a.m. or p.m., and keep listening while it waits for your answer. If you start by telling Alexa to set an alarm for 7:30 a.m., it shuts down after telling you the alarm is set. Checkmarx set the flag to remain open after Alexa gave the expected response in their malicious calculator app.

When the flag remains open, Alexa executes a function that prompts the user for the additional information it needs to complete the app. In the example, Alexa asks for clarification about whether the alarm should be set for the morning or evening. The prompt for further information tells the user that Alexa is still listening. The function that executes the prompt includes a variable that holds the text Alexa speaks when asking for the additional information. This variable will accept an empty string which allows Alexa to stay silent while it remains active waiting for the user to respond. The user asks the malicious calculator app a math question, gets the correct answer leading her to think the interaction is finished, and Alexa silently remains open waiting for the second response.

Now that Checkmarx had Alexa surreptitiously listening, they had to figure out a way to get it to record whatever it heard. Apps normally work by specifying a sentence format that has slots for user-generated input. For example, a set-an-alarm app might be configured as "Set an alarm for {Time}". The sentence structure is pre-defined and input for the slot is limited to a closed set of allowable words. Thus, the Time slot in the alarm app will only accept numbers that indicate possible times.

With Checkmarx's hack, Alexa wakes up and launches a malicious app, gives the benign response that was requested, remains active without prompting the user for more information, and records whatever it hears.

Checkmarx couldn't disable the blue light that Echo devices display when Alexa is active. If users notice the light, they'll know something is wrong. That's the good news. The bad news is that users don't always notice, Echo devices can be placed where the light is hard to see, and Alexa is present in an ever-increasing number of IoT devices that don't always include a visual indication that the device is listening.

After it hacked Alexa, Checkmarx notified Amazon and the two companies began working together to make it difficult for malicious actors to take advantage of the vulnerability Checkmarx had exposed.

- Bharathi V(VI Semester)

According to a study in 2013, each day 30000 servers get hacked. While in the 90s, hackers used virus, nowadays they rely on 'bots'

Applying Machine Learning to Cyber Security Analytics

When we look at the cyber security industry, we see two trends that lead us to the conclusion that machine learning approaches are a good fit for the industry. One, the collection and storage of large amounts of useful data points is already well underway in cyber security. It would be difficult for us to find a security analyst who is not currently overwhelmed by the vast amount of raw data that is collected every day in mature environments. There even exists a plethora of tools designed to help sort, slice and mine this data in a somewhat automated fashion to help the analyst along in their day-to-day activities.

The second trend is the lack of qualified, experienced individuals to successfully defend vital infrastructure and systems. Given these two points, machine learning techniques are a great fit to improve the security posture of an organization.

With a machine learning approach, many of the tasks can be automated, and even deployed in real time to catch these activities before any damage is done. A well-trained model would be able to identify new samples of malware that can evade human generated signatures, and perhaps quarantine the samples before they can even execute.

Currently, a large majority of machine learning approaches in cyber security are used as “warning” systems. They often require a human in the loop to make the final decision. This requirement is usually the result of machine learning models that are not sufficiently accurate, to the point where a typical human analyst is more accurate. As a result, the analyst has the final decision due to their lower false rates.

But what we are starting to see, and projecting to become increasing common, are machine learning systems that are in fact more accurate than their human counterparts. This is happening due to not only the improvement in machine learning, but also to the difficulty in growing the cyber security analyst human talent pool. Machine learning can help businesses better analyze threats and respond to attacks and security incidents. It could also help to automate more menial tasks previously carried out by stretched and sometimes under-skilled security teams. The massive amounts of data that are being generated, along with the problems of conducting large scale analysis to find the proverbial needle in the haystack, can be successfully solved using machine learning architectures.

- Ganesh Kumar M (VIII Semester)

The Enigma

The Enigma machine is a piece of spook hardware invented by a German and used by Britain's codebreakers as a way of deciphering German signals traffic during World War Two. It has been claimed that as a result of the information gained through this device, hostilities between Germany and the Allied forces were curtailed by two years. Arthur Scherbius, a German engineer, developed his 'Enigma' machine, capable of transcribing coded information, in the hope of interesting commercial companies in secure communications. In 1923 he set up his Chiffriermaschinen Aktiengesellschaft (Cipher Machines Corporation) in Berlin to manufacture his product. Enigma allowed an operator to type in a message, then scramble it by using three to five notched wheels, or rotors, which displayed different letters of the alphabet. The receiver needed to know the exact settings of these rotors to reconstitute the coded text. Over the years the basic machine became more complicated as German code experts added plugs with electronic circuits.

How the Enigma machine worked?

When a plaintext letter was typed on the keyboard, an electric current would pass through the different scrambling elements of the machine and light up a ciphertext letter on the "lamp board". What made the Enigma machine so special was the fact that every time a letter was pressed, the movable parts of the machine would change position so that the next time the same letter was pressed, it would most likely be enciphered as something different. This meant that it wasn't possible to use traditional methods to try and crack the notorious cipher.

To make things even more difficult, different parts of the machine could be set up in different ways, with each setting producing a unique stream of enciphered letters. Unless you knew the exact settings of the machine, you couldn't decipher the messages.

Deciphering Enigma

When the Enigma machine is used, the Enigma machine itself is the algorithm; the way in which it is set up is the key. Just as with any other type of cipher, as long as the recipient knows the key, the process of deciphering an Enigma encrypted message is incredibly simple. A German soldier receiving an enciphered message simply had to type the ciphertext letters into his own Enigma machine. If his machine was set up exactly in the same way as the message sender's, then the plaintext letters would appear on the lamp board. However, just as with any other type of cipher system, if you don't know the key it is very difficult to read the message - even if you know which system was used to encipher it.

- Sachin V Murthy (VI Semester)

Where Did Mark Go Wrong?

If you're one of those people who loves reading news every day and have a grasp on what's happening around the world, then I'm sure you would've come across the so called "data scandal" that's been going around. What makes all of this worse is that this crime is said to have been committed by none other than Mark Zuckerburg, whom most of us look up to, for the amazing person that he is. Sure, not all of you would agree with me on this. But looking from the technology perspective, the way the website and the mobile app is developed is nothing short of a huge success. Now what exactly was this data privacy all about? Was Mark really the one to be blamed here?

Whenever we create an account, be it on Facebook or any other website, as a new user? You enter your personal details! This can include things such as your name, your email ID, setting your password, and a few other things. For authentication purposes, these details are a must. But why would anybody want to give away their personal data to someone they don't even know, right? The web or mobile app developers who have built that application can easily access this data and can invade your privacy. This is where these people promise that the users' data will be kept private and will not be disclosed to any third-party service providers.

During the summer of 2014, the U.K. affiliate of U.S. political consulting firm Cambridge Analytica hired a Soviet-born American researcher, Aleksandr Kogan, to gather basic profile information of Facebook users along with what they chose to "Like." About 300,000 Facebook users, most or all of whom were paid a small amount, downloaded Kogan's app, called This Is Your Digital Life, which presented them with a series of surveys. Kogan collected data not just on those users but on their Facebook friends, if their privacy settings allowed it — a universe of people initially estimated to be 50 million strong, then upped to 87 million. The app, in its terms of service, disclosed that it would collect data on users and their friends. Kogan did have the permission to collect data, as Facebook allows application developers to gather data within its framework. However, Kogan mentioned that he's collecting the data for research purposes, when his intentions were something else. Cambridge Analytica is a company that "uses data to change audience behavior," both commercially and politically, according to its website. Its London-based affiliate, SCL Group, has a history of dubious tricks in elections around the globe. Cambridge Analytica worked in support of the 2016 campaigns of Trump, Ted Cruz and Ben Carson, all Republicans. Reports claim that Cambridge Analytica used data from Kogan's firm to help Trump win the elections, although the company flatly denies this fact. Reports also claim that the personal data of these 87 million people have still not been deleted and is still at stake. Imagine giving away your personal information to people who can manipulate with it, isn't that horrible? Due to these issues, more and more people started hating Mark Zuckerberg, and in fact, many people even deleted their Facebook accounts.

Ever since this incident, Facebook has changed its privacy policies and is focusing more on securing peoples' data. Is it too late? Will people stop using Facebook? Only time can tell us. The people at Facebook should've been more careful from the beginning. Mark should've never allowed other application developers to access data of the users of the Facebook app. According to me, this is where he went terribly wrong. It's high time Mark takes severe action and ensure that another incident like this never takes place.

- J Shesha Shankar (VIII Semester)

A Storage Area Network (SAN) solution combined with virtualization would offer higher availability

WPA 2 Protected? Well… It Can Still Be 'Krack'-Ed

It wouldn't be wrong to claim that internet is now an essential part of a person's life. Everything from entertainment to completing work can be accomplished using the internet. This dependency on the network made us find innovative ways to access the internet apart from wired methods.

WiFi is one such popular method of accessing the internet without having a physical connection to it. This eventually led to a requirement of having to secure this communication. Various standards evolved each being defeated by IT advancement. The most commonly used protocol to secure a WiFi network is WPA 2 security protocol. (As of 12/04/2018). WPA 2 is a security protocol which is an upgraded version of WPA. Previously, WPA was used with TKIP (Temporal Key Integrity Protocol) to secure a wireless network. WPA 2 supports CCMP which is an AES based encryption making it much stronger than WPA. WPA 2 was harder to set up for consumers who were not tech savvy or didn't have time to set up their WiFi properly. This led to development of WPS (WiFi protected Setup) to make it easy to set-up your wireless network. So how can we hack into a WPA 2 secured network? Well, with KRACK of course. KRACK is an acronym for Key Reinstallation Attack. They have performed successful tests on popular devices like Android, Linux, Apple, Windows, OpenBSD, MediaTek and Linksys to name a few. KRACK targets the 4-way handshake used in WPA 2. In a key reinstallation attack, the adversary tricks a victim into reinstalling an already-in-use key. This is achieved by manipulating and replaying cryptographic handshake messages. When the victim reinstalls the key, associated parameters such as the incremental transmit packet number (i.e. nonce) and receive packet number (i.e. replay counter) are reset to their initial value.
Essentially, to guarantee security, a key should only be installed and used once. By manipulating cryptographic handshakes, one can abuse this weakness in practice.

To patch this, individual manufacturers will have to deploy separate patches which are specific for that particular smart device or router. A lot of modern, tier 1 equipment is protected from this attack with recent fixes but a majority of networks are still vulnerable and hence this is NOT a redundant method at the time of writing.

- Ujjanth arhan (IV Semester)

Types of Data Security

The internet symbolizes a vulnerable route for trading data and information leading to a risk of attack or scams, like phishing. For the transferring of data much more methods have been used such as encryption or security.
There are several types of security, such as:

1. Network layer security

TCP/IP (Internet protocol) can be made protected along with the cryptographic techniques and internet protocols that have been designed for protecting emails on the internet. These techniques of protocols consist of SSL and TLS for the traffic of the website, PGP for email and for network security contains IPSec.

2. IPSec Protocol

This method is developed for protecting interaction in a protected way using TCP/IP. It is a setup of security additions designed by the IETF, and it gives security and verification on the internet protocol part by using the method of cryptography. The information is modified using security methods.
The two main aspects of modification that form the reasons for IPSec:

a) Authentication Header (AH) and Encapsulating Security Payload (ESP)
b) Portable Data Security

3. Email Security

When the customer completes writing the message and delivers it, the messages modified into a reliable format.
Using a connection of the network, the user of the email, modified to as a Mail User Argent (MUA), joins to a Mail Transfer Argent (MTA) running on the email hosting server. The email customer then provides the sender's identification to the hosting server. Also using the commands of the email hosting server, the users deliver the receiver list to the email hosting server.
The customer then sends the message. Once the server of the mail gets and procedures the messages, several issues occur: receiver hosting server recognition, establishment of connection and message transmitting. By using the Domain Name Server (DNS), the mail about the sender hosting server decides the email server for the recipient. Then, the hosting server reveals up a connection to the receiver email server and delivers the messages containing a procedure similar to that used by the coming customer, providing the recipient messages

-Ankit Anil Kulkarni (VI Semester)

RC4 is a proprietary, variable-key-length stream cipher invented by Ron Rivest for RSA Data Security, Inc.

MCQ – Praveen P B (VIII Semester)

1. A __________ is anything that can cause harm.
(A) Vulnerability (B) Phish (C) Threat (D) Spoof

2. A __________ is a small program embedded inside of a GIF image.
(A) Web bug (B) Cookie (C) Spyware application (D) Spam

3. A hacker contacts you on phone or email and attempts to acquire your password.
(A) Spoofing (B) Phishing (C) Spamming (D) Bugging

4. The phrase __________ describes viruses, worms, Trojan horse attack applets, and attack scripts.
(A) Malware (B) Spam (C) Phish (D)Virus

5. A hacker that changes or forges information in an electronic resource is engaging in __________.
(A) Denial of service (B) Sniffing (C) Terrorism
(D) Data diddling

6. The __________ of a threat measures its potential impact on a system.
(A)Vulnerabilities (B)Countermeasures
(C) Degree of harm (D) Susceptibility

7. What type of symmetric key algorithm using a streaming cipher to encrypt information?
(A) RC4 (B) Blowfish (C) SHA (D) MD5

8. To hide information inside a picture, what technology is used?
(A) R ootkits (B) Bitmapping (C) Steganography
(D) Image Rendering

9. What is the purpose of a Denial of Service attack?
(A) Exploit a weakness in the TCP/IP stack
(B) To execute a Trojan on a system
(C) To overload a system so it is no longer operational
(D) To shutdown services by turning them off

10. How is IP address spoofing detected?
(A) Installing and configuring an IDS that can read the IP header
(B) Comparing the TTL values of the actual and spoofed addresses
(C) Implementing a firewall to the network
(D) Identify all TCP sessions that are initiated but does not complete successfully

Answers:

1	2	3	4	5	6	7	8	9	10
C	A	B	A	D	C	A	C	C	B

Workshops and Technical Talks

A technical talk was organized on "World of compilers, trends and techniques" by Dr.Darius Blasband, CEO of Raincode Labs, Belgium on March 28th 2018 under ACSIS (Association of Computer Science & Information Science & Engg.). Dr. Darius explained to students about software immigration and the techniques used in compiler design by Raincode Labs.

A technical talk was organized on "Data Center Infrastructure Components & Technologies" followed by distribution of mementos to distinction holders in the VTU examinations on April 10th 2018 under ACSIS (Association of Computer Science & Information Science & Engineering). The chief guest Mr. Manjunath B.R, Manager Systems/Software Hewlett Packard Enterprise, focused his talk on Data Center Infrastructure Components, Data Center Infrastructure Management (DCIM) and Technologies used to develop DCIM Software.

A technical talk was organized on "Introduction to Machine Learning and the business drivers behind the use of Machine Learning" on April 27th, 2018, by Mr. Siddharth Roy, Senior Software Engineer, Siemens Corporate Technology, Bangalore under ISEA (Information Science & Engineering Association).
Mr. Siddharth discussed with the students the reasons for current focus on ML, namely the need of high computing power to handle huge amounts of data. This technical talk provided the students basic understanding of ML and insight on identifying the areas in business/industry and society where ML is applicable.

Business leaders consider cyber-security as a threat more now than ever before

Student Achievements

- Rajalakshmi K R has secured 1st rank in M.Tech VTU Exam 2016-17.
- Anusha V has secured 4th rank, Akanksha Bharadwaj has secured 6th rank and Neetu Purba has secured 7th rank in the VTU B.E. Exam 2016-17.
- Ron Astle Lobo, Shridhar Suresh Bhat, J Shesha Shankar under the guidance of Mrs.S. Srividhya , Assistant Professor, Dept. of ISE has won 2nd prize in Techorizon'18, National Level Project Exhibition and Conference for the project titled "Development of Tourism Information System using Content-Based Filtering," on 19th May 2018 at New Horizon College of Engineering, Bangalore
- Ron Astle Lobo, Shridhar Suresh Bhat, J Shesha Shankar have won the "Best Project" award for the year 2017-18 for the project "Development of Tourism Information System using Content-Based Filtering".
- Skanda Prasad and Rakshith G M of IV semester has won 1st place in IEEE Quiz on 27th April 2018.
- Sumukh Venugopal of VI Semester has won Gold medal in Indian Group Song, VTU Youth Festival 2018.
- Akshay Anand of VI semester has won RAGA LAYA PRABHA AWARD by Karnataka Kalashree on 13th May 2018.
- Hiranmayee S Dixith of IV semester has won 1st place in group song, VTU Youth Festival 2018.
- Sudarshan Rao M of VI semester has won bronze medal in skit, VTU Youth Festival 2018.
- Thanusha S.P. of VIII semester has won Gold medal in 50m and Bronze medal in 30m at interzonal VTU archery tournament.
- Thanusha S.P. of VIII semester has been awarded as the "Best Outgoing Student" for the year 2017-18.
- Ganesh Kumar M has won the "Best Presentation" award for the year 2017-18 for the presentation on the project "Object Recognition using Convolutional Neural Networks".
- Divya Kumari Gadhaiya has won the "Best Presentation" award for the year 2017-18 for the presentation on the project "Detection and Classification of Android Malware Apps".
- Aditya Vivek of VIII semester is the cultural ambassador of the year 2017-18
- Nikhil L and Thanusha S P of VIII semester are the sports ambassadors of the year 2017-18.
- Ujjanth Arhan of IV semester was in the team which developed an app for Arohan 2018 conducted by Department of MBA.

Editorial Team

Faculty

Ms. K M Bilvika,
Assistant Professor, ISE

Ms. Harini S,
Assistant Professor, ISE

Mrs. Madhura Prakash M,
Assistant Professor, ISE

Students

Sanchitha Thanay - VIII Sem
Nagashree H S - VIII Sem
G A Priyanka - VI Sem
S G Aditya Bharadwaj – VI Sem
Sanjana P S - IV Sem
Malavika S T - IV Sem
Rakshith G M - IV Sem
Mithun R - IV Sem

Email your suggestions to bnmit.ise.newsletter@gmail.com

It takes most business about 197 days to detect a breach on their network
Footer Facts by: Nagashree H S, VIII Semester