PROSENSE

175

Volume 6

Science & Technology

Compiled by
Prime Point Srinivasan
Dr. R Jagannathan
Priyadharshni Rahul

Prime Point Foundation | Chennai

First published June 2015
Second Revised Edition June 2016
Third Revised Edition March 2018
Fourth Revised Edition August 2019
Fifth Revised Edition September 2021
(in 8 volumes)

ISBN 978-93-91803-28-5

Pages 138
Price:

Publishers: Prime Point Foundation
www.primepointfoundation.in
www.corpezine.com
editor@corpezine.com

*****

Table of Contents

Introduction

Foreword From Dr. APJ Abdul Kalam For The First Edition PreSense100

Dr. A.P.J. Abdul Kalam
Former President of India

10, Rajaji Marg
New Delhi-110011

FOREWORD

I am very happy to know that the PreSense monthly ezine published by Prime Point Foundation is bringing out a book based on some of the unique articles, interviews and events published in its editions so far since from March 2006. The 100 issues of the publication have gone through an eventful journey, focusing on knowledge capture and important knowledge dissemination. I recollect my direct association with PreSense in July 2008, when I launched the cartoon character, 'Prince', created exclusively for PreSense.

I see PreSense continuing in its journey under the mentorship of Prime Point Srinivasan, maintaining its status as a must-read ezine, in the fast moving and evolving world of communication, knowledge and connectivity.

I congratulate the Editorial Team of PreSense for bringing out the 100th Edition as a Collector's Digest.

28th May 2015

(A.P.J.Abdul Kalam)

Preface to the First Edition

The emergence of Internet in the 1980s changed the way of communication globally. When Videsh Sanchar Nigam Limited (VSNL) introduced the internet for commercial use on 15th August 1995, India too adopted the new communication model and medium.

Way back in 2002, we published our first electronic newsletter in a move that was viewed as progressive and visionary in nature. After 8 issues, we had to discontinue the newsletter as its electronic form was not regarded contemporary then. In March 2006, we resumed with an ezine titled 'PreSense' with a shift in focus to creating awareness about the essence in personal and corporate communication.

Interestingly, at that time, no bigwig was willing to give an exclusive interview for the re-launching ezine, or even launch it, as there was apprehension about the success of the concept of an electronic magazine. Dr Y S Rajan (co-author of the book, India 2020, with Dr APJ Abdul Kalam) however encouraged us and volunteered to launch the ezine online.

And so we progressed, introducing interesting interviews with eminent personalities recorded on podcast and synchronised with the ezine format, so that the readers were treated to both online reading of contents as well as audio version of interviews. This enabled the readers to a feel of listening to the personalities they have read about in the ezine. We also introduced the concept of Guest Editorship, enabling the association of renowned professionals to share their experience and viewpoints as Editor for the month. This move gave an uplift to the outlook of the ezine and a new trend in its journey ahead.

Many newsletters and ezines launched during the same period were discontinued later for various reasons. PreSense however, survived the test of time and continued till its 60th edition in February 2011. After a deliberate brief break of a few months, we resumed the publication of our ezine, with a new look and a shift again in the focus to a social and general theme, with the tagline,

'Spreading Positive Vibrations'. This shift in focus enabled a more holistic approach to the theme and subject of communication. The attention moved to global current news, historically significant events, and knowledge-based breakthroughs in technology. This turned out to be an exciting challenge for the editorial team to sustain the positive strain while including novel and currently interesting topics for the reading pleasure.

Although an ezine might not be comparable with a giant-sized main line medium of communication, it has its own advantages as a medium of reaching out. The *Sansad Ratna* Award Scheme and the Education Loan Task Force were two major initiatives by our ezine, giving it the privilege of being recognised as the host to two major issues of national relevance.

Over a period of 9 years, our ezine has given opportunities to many young people to experience firsthand, the nitty-gritty of digital magazine making, editing and publishing. At the request of many of our loyal readers, we are now bringing out this book called 'PreSense 100', containing 100 plus articles, handpicked from the past 99 editions of our ezine. We felt that the selected articles qualified as a collector's item, and hence this special issue is described as a Collector's Digest. It is our belief that the reader too will appreciate it as one.

Up until now, our ezine has been published, not for commercial gains. We are proud to have many professionals on board, contributing their valuable time and talent in the making of the ezine every month.

I place on record my gratitude and appreciation to all the past Editorial Team Members like Satish Naaraj, Vidya, Tushar Panchal, Veena Vinod, Swetha and innumerable others who contributed immensely to make the ezine a professional one.

I personally thank our ezine's Editorial Team members for their sustained support in bringing out this book. I acknowledge the valuable support given by Susan Koshy, V Rajendran, T N Ashok, Prof. Jagannathan, Sukruti Vadula and Dr Ramamurthy Natarajan for editing and formatting this book.

At this stage, it is pertinent to mention that during the process of publishing every edition of the ezine, there was the collective, professional and committed involvement and input of every editorial team that was associated then. It has been the endeavour of the team to maintain a progressively high standard of the contents and readability of the ezine. We believe these efforts met the expectations of the readers, based on the positive and constructive feedback we kept receiving from our diverse and loyal readership base.

Right from the beginning, we have always been the beneficiary of the blessings and guidance of Dr APJ Abdul Kalam, Former President of India. I also thank Mr V Ponraj, (Scientific Advisor to Dr Abdul Kalam) who supported us in the selection of its contents.

When we planned to publish this book for free distribution, Dr Maria Zeena of Sathyabhama University volunteered to sponsor the cost. I thank her and her team for the noble gesture. I thank Polaris (Padmini and her team) for designing the cover. I thank Sri Logeswari Prints and its owner, Shri M Muthaian for bringing out this book on time.

I thank the innumerable readers and well-wishers who have given unstinted and close-knit support during our journey. Finally, I thank God Almighty for the divine blessings during the journey of 100 editions.

K Srinivasan
Chairman, Prime Point Foundation
Editor in Chief, PreSense

*****

Preface to the Second Edition

The First edition of PreSense 100 was released in June 2015 as a digest of articles published in the earlier 99 editions. The first edition received an overwhelming response from multifarious groups as students, IAS aspirants, parliamentarians, bureaucrats, and other intellectuals. In view of the support received from the readers, our editorial team decided to come out with the second enhanced edition titled PreSense 100+ with additional articles published between June 2015 and April 2016.

We thank Dr P Ganesan, Chairman of Sony Fire Works (Pvt) Limited and AAA College of Engineering and Technology, Sivakasi who volunteered to sponsor and print this second edition for distribution. The Editorial Team gratefully acknowledges the support given by Shri Bharath Matha Mohan (Educationist at Chennai) and Shri VSM Velmurugan (Chairman of VSM Groups, Kovilpatti) in bringing out this second edition. We also thank Smt. Padmini and her team at Intellect Design for designing the wrapper. We thank innumerable other people who contributed to make this second edition possible.

K. Srinivasan
Editor in Chief
PreSense

*****

Preface to the Third Edition

The first edition of the Digest titled PreSense 100, containing articles published in the first 100 editions of our ezine was released in June 2015. The second enhanced edition titled PreSense 100+, covering 110 editions, was released in June 2016. Due to the overwhelming response from our readers, we are now bringing out the third enhanced edition, covering important articles published in 130 editions of our ezine PreSense. This Digest is titled PreSense 130.

Dr P Ganesan, Chairman of Sony Fire Works (Pvt) Limited and AAA College of Engineering and Technology, Sivakasi has always been a source of inspiration to us. He sponsored the second edition of Digest. This time too, he has volunteered to sponsor and print this third edition for distribution among youth.

We also thank Smt. Padmini and her team at Intellect Design for designing the wrapper. We thank innumerable other people who contributed to make this third edition possible.

K. Srinivasan
Publisher & Mg. Editor
PreSense

*****

Preface to the Fourth Edition

The journey of the eMagazine PreSense since March 2006 is amazing and exciting. During this journey, we were able to publish in the print format three editions Digest of articles published in the 100,110 and 130 issues respectively.

We have been receiving large number of appreciation from readers on the contents of Digest. Enthused by this, we are now pleased to release the fourth edition of digest in digital format titled PreSense150 containing select articles published in the 150 issues.

We thank Dr B Muthukumaran, Co-Founder of Digital Security Association of India (DiSAI) and Advisor to Digital Journalists Association of India (DiJAI) for all technical support in making this eDigest. We also thank Smt. Padmini and her team at Intellect Design for designing the wrapper.

I personally place on record my gratitude to Mrs Susan Koshy, Mr Rajendran, Mr Triambak Sharma and other editorial team members for the sustained support they are giving for successful publication of the eMagazine PreSense every month. We thank innumerable other people who contributed to make this third edition possible.

K. Srinivasan
Publisher & Mg. Editor
PreSense
24 August 2019

*****

Preface to the Fifth Edition

The eMagazine PreSense which was started in March 2008 on the suggestions of Dr APJ Abdul Kalam for positive journalism has reached the 175th edition in September 2021. This digital only eMagazine is passionately run by a group of eminent volunteers without any commercial motive and without accepting any advertisements.

Looking back, we have published high quality articles on various subjects, including current affairs in every issue. Earlier, we have published Digest of articles after 100, 110, 130 and 150th editions. We had the great honour of getting the Foreword from Dr Abdul Kalam himself for the first Digest published at the end of 100th edition.

This is the fifth Publication at the end of 175th edition. Earlier, we provided all articles in a single book. Due to the large number of important articles, we have grouped all the articles in 8 categories. We are now publishing PreSense175 in 8 volumes covering (1) Indian Heritage, (2) Spotlights from History, (3) Politics and Governance (4) Prince cartoons (5) Media and Communication (6) Science and Technology, (7) Health and (8) General and Exclusives.

I am thankful to Priyadharshni Rahul (Editor), T N Ashok (Consulting Editor), Dr R Jagannathan (Editorial Advisor) and Srinivas Gopal (Technology Advisor) who helped in compiling the select articles published in the past editions.

K. Srinivasan
Publisher and Managing Editor
PreSense
26th September 2021

Journey of Ezine PreSense - Milestones

Dec 1999	Launch of Prime Point Foundation, Publisher of the ezine.
Feb 2006	Launch of ezine, PreSense online by Dr Y S Rajan.
Aug 2006	Integration of Podcast with the ezine contents.
Aug 2007	Introduction of Guest Editors.
Feb 2008	Second Anniversary Edition with Dr Abdul Kalam's exclusive interview. Masthead changed.
Apr 2008	First ezine to become 'Media Partner' for a global event held at London.
July 2008	Introduction of cartoons – Cartoon Character 'Prince' launched by Dr Abdul Kalam.
Sep 2008	Change in layout, introducing photographs on the cover.
Jan 2010	Ezine's new initiative 'Education Loan Task Force' (ELTF) launched to create awareness among students and parents.
May 2010	Ezine's second initiative to honour top performing Parliamentarians, with the *Sansad Ratna* Award launched. Golden Jubilee (50th) Edition launched.
Feb 2011	Diamond Jubilee (60th) Edition.

A hiatus after 5 years of uninterrupted journey

Apr 2012	Ezine resumed in a new format of contents. The tag line changed from 'Communicate the Communication' to 'Spreading Positive Vibrations'.
Apr 2013	Tamil Nadu Governor launched a special edition on the Indian Parliament, coinciding with the *Sansad Ratna* Awards.
Jun 2013	Platinum Jubilee (75th) Edition launched by the youth at three places simultaneously, across the nation.
Jun 2015	100th Edition - PreSense 100 released in print format.
Mar 2016	Ezine's third initiative 'Digital Journalists Association of India' (DiJAI) launched.
Jun 2016	Second edition of PreSense 100+ released in print format

Dec 2017	Ezine's fourth initiative 'Digital Security Association of India' (DiSAI) launched.
Mar 2018	Third edition of Digest PreSense130 released in print format.
Aug 2019	Fourth edition of Digest PreSense150 launched in pdf format.
Sep 2021	Fifth edition of Digest PreSense175 in 6 volumes released.

The Journey Continues…..

*****

Editorial Board – October 2021

PRIME POINT Foundation

Prime Point Foundation and its Initiatives

Prime Point Foundation, a Non-Profit Trust and NGO was founded in December 1999 by Shri K Srinivasan (popularly known as Prime Point Srinivasan), a former Senior Banker and a Digital Journalist and Communication Professional, to promote leadership and communication skills among the youth. Very eminent persons are associated with the Foundation.

In the past 21 years, the Foundation has organised several seminars, workshops, training and interactive sessions, both offline and online, on various subjects of national interest. The Foundation manages various online discussion groups and podcasts on communication, and digital journalism.

The Foundation has formed 5 initiatives to create awareness in various domains. All these initiatives are managed independently by passionate experts. These initiatives are non-commercial, and focussed on youth.

PreSense: The eMagazine PreSense was started in March 2006 on the suggestion of Dr APJ Abdul Kalam to promote positive journalism. Till September 2021, the Foundation has published 175 editions. This is a digital-only magazine. Digests, containing select articles upto 150 editions of the eMagazine, have so far been published. Dr Abdul Kalam has written the foreword for the Digest of articles upto 100 editions. PreSense publishes the cartoon character Prince, which was launched by Dr Abdul Kalam in 2008. PreSense will be publishing a Digest of select articles published upto 175 editions in the month of September 2021.

Sansad Ratna Awards: This is a flagship initiative started in 2010 to honour top performing Parliamentarians every year, based on various performance parameters, and selected by a Jury Committee of eminent Parliamentarians. Dr Abdul Kalam himself inaugurated the first edition of the Awards event in May 2010. Till 2021, the Foundation has conducted 11 editions and presented 75 Awards. IIT Madras was the supporting Partner upto the 9th Edition. 10th Edition was held at Raj Bhavan, Tamil Nadu. 11th Edition was held at Constitution Club of India, New Delhi.

Next Gen Political Leaders (NGPL) is an off-shoot of Sansad Ratna Awards. This is a registered NGO operating since 2018. NGPL has organised several workshops online and offline, for young political leaders and aspirants. Ministers, parliamentarians, legislators and retired constitutional authorities have participated and shared their views. NGPL will shortly be instituting Awards for young promising politicians.

Education Loan Task Force (ELTF) was started in 2010 to create awareness about education loans, among students and parents. More than 30,000 queries have been responded to, through email, and more than 5000 serious complaints have been taken up with the top management of the banks concerned, for redressal. Many policy issues have been taken up by Sansad Ratna Awardee MPs, in the Parliament for solution. ELTF does not facilitate loans.

Digital Journalists Association of India (DiJAI): DiJAI is an independent NGO founded in 2017 to create awareness about digital journalism and its implications, among the public and particularly among the journalists. DiJAI conducts several online and offline workshops and seminars, with panels of domain experts.

Science and Technology

What are Cyber Crimes?

Phishing is the process by which someone obtains private information through deceptive means of authenticating credentials, in order to assume someone else's identity. The phisher, viz. the person doing the act of phishing, sends an email and directs the victim to a fake web-site (which appear genuine, say like your bank's website) and advises the user to divulge his User ID for internet banking along with other private information like password, credit card number and possibly the 3-digit code number in the credit card (called the CVV or the CVC). With such information, the phisher then accesses the actual web-site and does an e-commerce or e-banking activity on the victim's bank account.

Skimming is the process of copying the magnetic strip information from a credit card into a small handheld electronic device, called skimmer (now available in the form of contactless and remote facility too). It scans and stores the card data from the magnetic strip. Such information is then passed on to the people engaged in the manufacture of counterfeit cards. With the name of the bank and the card-holder (already available at the shop, where the skimming was made), this information will then be embossed in the card and the card looks like original! Fraudsters then indulge in shopping (either in person or on-line) using the fake cards. The victim will get to know of it only after he receives the card statement from the bank.

Computer hacking is the act of getting into someone else's computer involving some degree of infringement on his privacy and causing damage to information like computer files or any software stored therein. Unlike most computer crimes and computer misuse which are clear cut in terms of actions and legalities like software piracy etc, hacking is a little more complicated to define and describe as an offence. Hacking may result in a simple invasion or annoyance to a computer, or to the extent of illegal destruction or compromise, affecting the information therein. Ethical hacking (which is now being taught as a subject) involves the use of technical knowledge by individuals, willing to take the risks required to become a true "hacker" to explore the weaknesses in

any system and confirm that the computer system is really robust enough to withstand any hacking attempt.

Spoofing means maliciously deceiving someone. IP Spoofing refers to the transmission of data with a forged (spoofed) source Internet Protocol address with the purpose of concealing the identity of the sender or impersonating another computer system, thereby duping the receiver to believing that the mail has been sent by the system whose IP address has been forged. Similarly, email spoofing refers to the act of sending an email to make it appear as if it came from somewhere or someone other than the actual one by altering the header information after connecting to the mail server.

Cyber Stalking means causing harassment to someone through the computer. Commonly reported forms of stalking include sending repeated emails or SMS to a victim causing mental disturbance or mental agony affecting the behaviour of the victim in a psychological manner. Similar to receiving obnoxious and objectionable telephone calls, the victim receives emails and SMS from the fraudsters, causing embarrassment that affects his mental health.

By V Rajendran, Editorial Team Member
Source: October 2008 issue of PreSense

*****

An Overview of Current IT Security Issues, the Future Trends and Possible Actions

1. Cyber Attacks

The Internet or World Wide Web (www) is also called Cyber Space. This space connects various computer networks across the World (and in future to the other planets that we might occupy!!). Like each individual, each network is distinct in terms of the IT systems used, the way it is set up, configured and managed. This heterogeneous nature of the network has many weaknesses that are prone to attacks. Cyber terrorism, cyber warfare and cyber vandalism are examples of such attacks. Many such attacks are happening today albeit less in magnitude and in the future, we may face some intensive attacks that could cripple the cyber space.

Co-ordina.

ted efforts from the Computer Emergency Response Teams (CERT) across the world with timely alerts to user communities could mitigate risks from this threat.

2. IT Vulnerabilities

Vulnerabilities in IT systems are holes or errors that are exploitable. They are there due to poor designing or poor coding or both. When the vulnerability is exploited, it results in security violation such as compromise of the IT system, service disruption or obtaining higher privileges. Such vulnerabilities are the root cause of many of the security issues mentioned in this column.

Efforts such as Common Vulnerabilities and Exposures (CVE), and National Vulnerability Database (NVD) provide a glimmer of hope for combating and reducing these threats in the future. Based on the knowledge from various hacking/virus/worm related incidents, it is possible to develop secure systems by following the secure coding practices.

3. Lack of Monitoring, Security Testing and User Awareness Programs

Though this is an organisational issue, monitoring of suspicious activities in the network, is performed using IT systems. Information Security is predominantly based on preventive and detective controls. Monitoring assists in devising proactive and

reactive actions, based on events. Security testing involves vulnerability assessment, penetration testing and security policy audits. The trends indicate that many organisations do not have or do not follow such procedures.

User awareness in terms of Do's and Don'ts based on organisational security policy must be created. These three activities, if followed regularly, could minimise the risks from the threats mentioned in this column.

4. Identity Theft

Identity theft refers to stealing one's identity for wilful gain such as money, fame, and power, and for criminal activities. A simple identity theft is stealing a password. Banks and financial institutions are defrauded by impersonation; confidential data are stolen from the Government, military and corporate for terrorism, warfare and espionage due to identity theft. In the future, this issue will assume gigantic proportions as more and more devices join the network bandwagon and establish their identity beside humans.

Digital Certificates, Biometrics such as finger print, voice, face and retina recognition systems, and Radio Frequency Identification Devices (RFID) are some of the effective solutions to this issue and we can expect advancement in this area.

5. Malware

Malware refers to (Mal)icious Soft(ware) and as the name implies, the purpose is to cause harm to the systems or steal information. Viruses, worms, and spyware such as key loggers, Trojan horses, root kits etc., are examples of malware. The present trend is alarming and statistics show that hundreds of billion dollars are lost due to malware.

Statistics show that more than 50% of online users have reported spyware infection to their systems. Malware exploits system vulnerabilities and human weaknesses. Organised crimes such as planting malware in legitimate websites as online banking, so that it gets automatically downloaded to the computers of the innocent users, are on the rise. Technologies like Web2.0 are also prone to malware infestations.

Future trends indicate the onslaught of more sophisticated malware, and there is need for heightened awareness, using the legal copy of the operating system, anti-virus and personal firewall by the users.

6. Botnet

Botnet refers to malicious networks managed by Computer Robots. They attack vulnerable computers (called zombies) in the network and use them for attacking other computers, stealing information, storing and transmitting illegal data such as porn movies or pirated and malicious software. We see proliferation of distributed botnets that automatically switches the controlling computer robot to another computer or network in case of network block by the service provider/law enforcement agencies. This trend is going to increase, and controlling botnets will be a big challenge. There is an unofficial estimation that one quarter of the computers connected to the Internet will be compromised and will become part of botnet. User awareness and periodical vulnerability and activity scanning of computers are necessary for combating this threat.

7. Unsolicited Commercial Email

Spam, as it is popularly known is an issue that drains the network resources such as bandwidth and storage space. Besides, many human hours are wasted in download time and trashing such emails. Important security issues are that spam is used for phishing, pharming and distribution of malware. The root cause of the problem is the way the email is transported and exchanged across millions of mail servers across the world and the weak spam controls. The present trend is more on using zombie computer to send spam as more and more service providers are shutting down spam servers. However, many of the spams originate from servers hosted in countries like Russia, China and Philippines.

Using spam filters, and co-ordination from the countries that do not have stringent laws against spam, is the way to go for solace from this menace.

8. Mobile and Wireless Attacks

The business and user community increasingly adopts mobile devices and wireless networks. Mobile commerce such as banking and shopping are seeing rapid advancements. Common attacks that are perpetrated against such devices and networks include Bluetooth Attacks, SMS Spoofing, Smishing (SMs phISHING), compromising the WEP keys as well as setting up ad hoc networks. In the future, attack sophistication and vectors are bound to increase and this is one area that is going to give a constant nightmare to IT and Security professionals.

User awareness is the key to prevent many such attacks besides stronger authentication mechanisms.

9. Web Based Social Engineering

Social engineering refers to the art of inducing a user to inadvertently perform an action for the purpose of obtaining sensitive information, such as passwords, credit card or bank account information etc. Web-based tactics involve spoofed emails that appear to have come from legitimate entity such as your bank, asking for personal details, Nigerian scam, illegitimate websites constructed as a lookalike of a legitimate site or in the form of giving away free software, music or video. With the advancement of social networking sites, instant messaging and mobile phone based internet communications are some of the hot spots that will spur this activity to dangerous levels.

People are the weakest link in a security chain. A common sense approach to any access or communication with known/unknown entity on the web must be practised.

10. Peer-to-Peer File Sharing

This refers to the direct communication between two or multiple computers for sharing files such as software, music, video etc. Since this activity involves direct access to the file system of the shared computer, the chances of implanting malware is very high. The concept of trusted source in such a system is weak. Criminal networks operate in the domains that perpetuate organised crime. The trends are more geared towards underground suspicious activities.

Participating in an insecure peer-to-peer file sharing networks must be avoided.

Law Governing Your Computer

Information Technology Act 2008 – India: Section 43A

Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected.

(There are similar provisions in other countries like USA and UK)

Source: April 2009 issue of PreSense

*****

Origin of Email

In 1965, Massachusetts Institute of Technology (MIT) was the first to demonstrate the use of the email system known as MAILBOX. This was before the internet came into existence and therefore, this system was used to send messages to different users on the same computer.

Ray Tomlinson

In 1971, Ray Tomlinson, a former MITian, was working on TENEX operating system as an ARPANET contractor for BBN Technologies. While using a local email program called SNDMSG, Tomlinson created the first email application when he patched a program called CPYNET to the existing SNDMSG. This introduced the capability to copy files through a network and Ray notified his colleagues by sending them the first email. It is said that the first message sent by Ray was 'QWERTYUIOP', which is formed by typing of characters on a keyboard. Mr Tomlinson sent this historic message to himself from one machine to another, sometime in October 1971.

The room from where Mr Tomlinson sent the first email message from one computer to the other. (Photo courtesy: http://tenex.opost.com/)

The history of email addresses can also be attributed to Tomlinson. He chose the '@' symbol to provide an addressing standard in the form of "user@host", which is in use till date. This is why Tomlinson is called the 'father of email' and is credited with its invention.

Source: January 2011 of PreSense

*****

Cyber Security Information Sharing - the US Initiative

The Cyber Security Information Sharing Act (CISA), originally introduced in July 2014 and under discussion ever since, was approved last month, after some modifications. It is now made easier for companies to share personal information with the government in case of cyber security threats in USA. The information-sharing channels in the US, created for responding quickly to hacks and breaches, along with intelligence and law enforcement agencies can now enforce surveillance without a warrant.

Since the cyber security threat information is shared, it is feared that the threat indicators can be used as evidences to prosecute cyber crimes. This is being condemned as an infringement on the data privacy of individuals in USA, with the privacy advocates opposing it. With the powers vested, the President can now set up 'portals' for agencies like the FBI and National Intelligences, and all such information could be used for law enforcement investigations.

In cyber security worlds, this is being considered a significant and landmark legislation in cyber crime prevention.

It is felt that an Act with similar provisions suitable to the Indian environment should be in place in India too. Alternatively, the Cyber Crime Co-ordination Centre should be operationalised at the earliest to help speedier investigation of cyber crimes and sharing of cyber crime related information among the main stake holder government agencies. More details are available in the following link.

https://www.congress.gov/bill/114th-congress/senate-bill/754

By V Rajendran, Editorial Team
Source: January 2016 issue of PreSense

*****

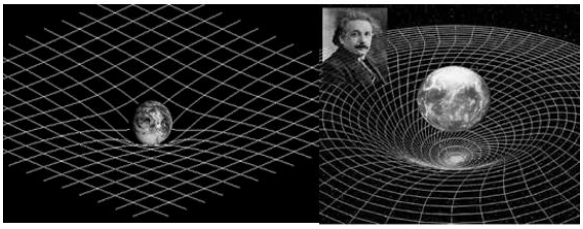
Gravitational Waves - Discovery of the Century

The announcement by the Scientists on 11th February 2016 about the discovery of 'Gravitational waves', the ripples in the fabric of space-time, electrified the world of astronomy and scientists. This is the discovery of the century as the gravitational waves were predicted by Albert Einstein in 1916. In 1979, National Science Foundation funded California Institute of Technology and Massachusetts Institute of Technology to detect the waves. They set up Laser Interferometer Gravitational Observatory (LIGO) detectors to conduct the study.

Prime Minister Narendra Modi lauded the role of Indian Scientists who were part of the team that discovered the 'Gravitation waves'. "The historic detection of gravitational waves will open up new frontier for understanding of universe. Hope to move forward to make even bigger contribution with an advanced gravitational wave detector in the country", he tweeted.

Gravitational waves explained

We know that a stone tossed up, falls back to Earth because of its gravitational force that draws the stone to the earth. We have the Newton's law to explain and measure the force of gravity. This explanation is sufficient for theoretical understanding. What really happens is the following:



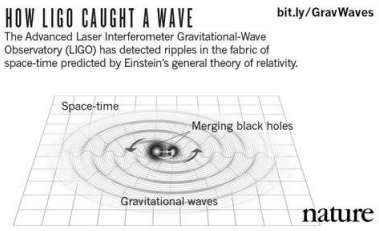
Imagine that two of us hold the four corners of a handkerchief so that the piece of cloth is now a plane surface. Now, imagine placing a very heavy iron ball at the centre of the handkerchief. The shape of the handkerchief gets curved as shown in the figure.

The curved space around a massive object like a star is called Space-Time fabric, since it is not just a change in length-breadth-

width that occurs. Time changes too in this curvature. Therefore, a stone thrown above the earth travels back through this curvature of space-time and ultimately touches the central massive body (Earth), an action we term as the stone falling back on Earth.

If the central massive object remains at rest, or moves at a steady and consistent speed, the curvature of the space-time remains at rest, or moves at the same speed. But if the central mass moves with acceleration, then the changes of curvature of this space-time fabric generates gravitational waves. These waves propagate in space at the speed of light.

Einstein predicted the existence of these gravitational waves in 1916 itself as a consequence of his General Theory of Relativity.



Detection of These Waves

About 1.3 billion years ago, two black holes, each having a mass of about 30 times our Sun, attracted each other and collided with each other producing intense gravitational waves. INTENSE means these waves have a wavelength measuring millions of miles but with a sub-millimetre height. To detect such an extremely weak gravitational wave, the Laser Interferometer Gravitational Observatory (LIGO) Team in USA made a pair of coherent laser beams to travel in mutually perpendicular paths of about 4 km each in length and recorded the changes in the path lengths by observing an unambiguous interference pattern when these gravitational waves were crossed in the observatory. Had Einstein been alive today, he would have been amazed at the technology that enabled this detection.

The Significance of This Discovery

- For the first time we have direct evidence of a black-hole, rather two black-holes of about 30 solar masses colliding with each other, as predicted by Einstein.
- The gravitational waves that are now detected matched exactly with what Einstein had predicted.

- Where Does This Discovery Lead Us To?
- Just as we have optical and radio telescopes to observe our Universe in-depth, we can now observe through gravitational-waves-interferometers, which can give us unblurred details.
- Our Universe has energy distribution roughly as follows: 68% dark energy, 27% dark matter and 5% normal matter.

Remember that we are all made up of normal matter and hence currently, we can perceive only this 5% of the Universe. With this discovery, we can now probe the dark matter too since they have "mass" and can give rise to gravitational waves.

We can see the Universe close-up to 2 or 3 seconds of its formation! The gravitational waves will pave the way to look in to such a nascent Universe. (please note that we are now able to look at the Universe only after 0.28 billion years of its birth).

Benefits to a Common man

When the experiment at European Organization for Nuclear Research popularly known by the French acronym CERN, Geneva, was organised to detect the "GOD" particle, the scientists had the necessity to interlink many of their research computers, which gave the world the "World Wide Web" (www). The LIGO Labs in India (to be established soon) can now bring distinct advantages to our scientists, researchers, students, the government and the entire country.

The precision of the measurements involved in the detection of gravitational waves are so high that

- early warning systems for disasters like tsunami will be absolute, correct and more reliable on the dot.
- analysis and understanding of DNAs at the bond-level is possible and this can throw more light in understanding healthy and diseased conditions, leading to stunning biological discoveries.
- it will give an unprecedented ability to process really big data, giving a direct advantageous edge – the following list is only

indicative and not complete – to our military, disaster management and crisis management.

Please watch this video to get the visual details.
https://www.youtube.com/watch?v=hhbMpe17fzA

By Dr R Jagannathan, Editorial Advisor
Source: February 2016 issue of PreSense

*****

Booking Domain Name for a Company

The head of a popular organisation in India, one day found that the domain name of his organisation was registered with some other person, who was handling its website management. A few months earlier, the head of the organisation had requested that web designer to book a domain name like *www.mydomain.com* and paid the charges. The web designer instead of booking the domain name in the name of the organisation, booked it in his name. When the head of the organisation requested the web designer to change the registration in the name of the organisation, he was reluctant to oblige. Since the domain, including the user ID and the password of the booking, is in the name of the web designer, the organisation has to depend on the web designer always.

As per the international guidelines of The Internet Corporation for Assigned Names and Numbers (ICANN), anybody can book the domain name with any extension, barring a few names. The commercial and non-commercial organisations run the risk of their full name or short name being used for domain name booking by any third person, on payment of the required charges. Here are a few tips for secure registration of the domain name, without the risk of being misused.

1. Select your domain name, like 'mydomain'. This name should be short, reflect your organisation and should be easily remembered.

2. Go to any domain booking registrar like Godaddy, Networksolution, Register, etc. Search for your domain name. If it is available, create an account with them with your full name, organisation, postal address, contact numbers, etc. Then you can

book your domain name online, paying the required charges through credit card.

3. Every domain name has three contact details viz. Registrant, Admin and Tech. Ensure that the name of your organisation is given as the contact detail for all the three contact categories. Even if you are advising the web designer to book your domain, advise him to book it only in the name of the organisation or the real owner, to avoid any future complications.

4. Once the domain name is booked in the name of the organisation, the web designer will need to visit the control panel of the domain name only when he has to change the DNS Settings or the Name Server Settings. The annual renewal charges can be paid online, when you receive the alert from the registrar.

5. Keep the user ID and the password of Domain Registrar safely and do not share them with others. Using the same user ID, you can book any number of additional domains.

6. To ensure against any misuse of the name of your organisation in the future, you can register several domain names with different connotations like *mydomain.com, mydomain.net, mydomain.org, mydomain.in, mydomain.co.in*, etc. All the domains can be pointed towards your main site. If yours are a popular company or organisation, and if you are holding only one domain name *mydomain.com*, another person can book a domain name *mydomain.in* and could create trouble for you. This kind of activity is called 'cyber squatting'. Since cyber squatting has not yet been categorised as an offence under the cyber law, the responsibility of protecting the domain name vests with the genuine owners.

parked whitehouse.com site

Interestingly, whitehouse.com is not with the American Government. It was used as a porn site earlier and now they have parked the site without content. Whitehouse.gov is the official site of the President of India. There are instances where several leading Indian organisations do not own domain names with other extensions. Such organisations run the great risk of mischief makers who might purchase these domain names, causing embarrassment.

After reading this article, please visit *who.is* and get the registration details of your personal and official domain names. If there are any discrepancies, you can rectify them immediately and safeguard the interest of your organisation and yourself.
Web designers have no moral or legal authority to book domains in their name on behalf of the organisation when you have asked him to book on your behalf.

V Rajendran, Editorial Team
Source: March 2016 issue of PreSense

*****

The Safety of Women in Cyber Space

Are Ladies Safe in Cyber Space?

A month ago, I received a telephonic call from a lady television anchor, informing me about the harassment she was facing from some people, who abused her on Twitter, using indecent language. She had saved the screen shots of those tweets. Rajendran, PreSense Editorial Team Member and a Cyber Advocate, and I suggested to her to file a complaint with the Cyber Crime Police. Last week, she called me up again to lament that in spite of her lodging a complaint with the Police with proof of the tweet screen shots and the names of the offenders, the Police was not sure how to deal with the case, in the absence of Sec 66A (of the Information Technology Act 2000), which was struck down by Supreme Court in March 2015. The Police across the country have been receiving such complaints regularly and they take action by invoking the Indian Penal Code (IPC) to book the culprits. She also said that there were many young girls being constantly abused in the cyber space of the social media. She added that some of them had to take extreme step of even leaving their jobs, unable to handle the harassment by the abusers.

She then raised a relevant question. "When I walk on the street, and if someone uses abusive language against me, the Police can arrest the offender under IPC for 'eve teasing'. If an offender does a similar offence in the cyber world, the law is handicapped to arrest the offender. How are you going to protect your sisters and daughters from this menace?" Her question, choked with emotion, prompted our Editorial Team to write this Cover Story.
We conducted a quick online survey to gain some insight into the extent and intensity of such cyber harassment. Based on the responses, we discussed the issue with many experts and activists on the subject.

Problems Faced by Women

In the survey, many of the women respondents complained about the abusive, indecent, derogatory and vulgar calls, messages and

images they received through mobile phone calls, the social media and the WhatsApp. All these abuses are called 'cyber stalking'.

One of the Chennai-based lady respondents reported that a photographer, whose services were engaged for her wedding, took some close-up pictures of her in suggestive poses. The photographer then posted one of those pictures on his Facebook page. When she got to know of this mischief, she complained to the Police. However, the police expressed helplessness in taking action against him, as the photographer was politically connected and used his political connections to avoid criminal action against him.
Recently, a senior male student of a reputed college uploaded some photographs of some girl students, on his Facebook page, displaying them with vulgar captions. When these were detected, the student was dismissed from the college and the pictures were removed from the social media page. The affected students and the college refrained from complaining to the Police to "safeguard their reputation".

In another instance, a male member of a software company proposed his love to his lady colleague, who rejected him. In revenge, the male colleague uploaded photographs of her on various porno sites, with her mobile phone number. She was displayed as a call girl, available for service. The lady colleague experienced acute embarrassment and agony because of his vengeful act. Many of the millions of daughters of India, who are harassed on a daily basis, suffer in silence. Many of them do not go to the Police, and instead tolerate the harassment as their "fate".

Section 66A of Information Technology (IT) Act 2000

In 2009, the Government of India inserted Section 66A in the Information Technology Act 2000, empowering the Judiciary to punish a person with imprisonment up to three years for any grossly offensive and menacing messages. Unfortunately, in a "twist in the tale" episode, a lady law student challenged this Sec 66A as unconstitutional because this section was misused by the police in one of the states to arrest innocent persons who posted

critical comments about social and political issues and political leaders on social networking sites. The Supreme Court thus struck this section down, saying such a law "hit at the root of liberty and freedom of expression, the two cardinal pillars of democracy".

The entire media in India, including several women organisations celebrated this decision as winning their newfound 'freedom of expression'. Many others, who were less optimistic about the wisdom of this reversal, remained silent. The Cyber Society of India however, had expressed openly in the media that striking down Sec 66A might open threatening challenges for women in the future, compelling them to ask for re-introduction of this provision.

Expert Views

S. N. Ravichandran of Cyber Society of India says that the right of redressal has been sacrificed at the altar, for the sake of the right of speech and expression. He adds that at the time of the judgement, he had appealed to the women journalists and women activists to oppose the judgement. None of them seemed to realise the implications then.
Sonia Arun Kumar, a popular Digital Journalist says the Government should restore Section 66A to protect the women victims.

Dr.Debarati Halder, advocate and cyber crime victim counsellor, says that Sec 66A was a good law that was unfortunately misused and abused. She feels that the existing laws are not adequate to address the many forms of cyber offences, even though some of them can be tackled through IPC.

S. Balu, Additional Superintendent of Police (Retired), who investigated a similar case of harassment on cyber space and won the first conviction in India under IT Act, says that the Police feels handicapped to take action against the offender due to the absence of the Section 66A. There are many laws in India that are being misused on a daily basis in many parts of India. Striking down those laws is not a solution. The Court could have directed the Government to frame rules to prevent misuse, instead of striking down the section.

Balu quoted a case of the recent conviction of a software engineer, who indulged in Cyber Stalking before the introduction of Section 66A. He was convicted by the Court under Section 67 of IT Act (punishment for publishing obscene material in the electronic form) and Section 509 of IPC (uttering any word or making any gesture to insult the modesty of a woman). However he feels that 509 IPC which was framed in 1860 does not take into consideration the activities in cyber space. "The new situation warrants a new law", he adds.

Naavi, Founder of the online Cyber Law College and the author of the first book on Cyber Law in India also agrees that Sec 66A should not have been struck down, exposing the Indian women to greater risk. He pleads that a new section be brought to replace Sec 66A. He wants the media and the woman organisations to take up the matter with the Government.

What Victims Should Do?

Before filing a police complaint, the women, harassed through the mobile phone, Facebook, Twitter or any social medium, can first warn the culprit of dire legal consequences. In 90% of the cases, the culprits will not trouble the victim thereafter. If the culprit pursues with the harassment, the victim can file a police complaint, providing evidence of the harassment. If the Police does not respond, the victim can pursue through women social organisations. They can also approach the courts to issue directives to the Police for action.

In the case of harassments turning serious, the victims should also approach the National Human Rights Commission and National Commission for Women for redressal of their grievance.

Why Protection to Women?

Ravichandran feels that women should understand that their protection begins by taking care of themselves first. It does not make sense to talk of gender equality and then seek safety and special protection in the same breath. However Sonia, representing the current youth, feels that with the growth of technology and employment opportunity, women are not confined indoors and are exposed to the risks of encountering perverts in the society. While the Constitution provides equality to all, we as a society, must provide social justice and protection to the vulnerable sections of the society.

The women community is one such vulnerable section of the society which needs to be protected by the responsible society, from miscreants. These women are the daughters and sisters of the society. Sonia feels that all elders in the family and the community should counsel the boys and sensitise them towards treating women, irrespective of their age and social background, with respect and dignity, as they hopefully, would treat their own sisters.

Though the elders may sound conservative, the hidden concern cannot be ignored. While every effort has to be made to make the law tighter, we should understand that the law in the statute books alone cannot resolve this issue. The individual and the social system should develop inherent strength to face and deal with the challenges.

By K Srinivasan, Editor in Chief
Source: April 2016 issue of PreSense

*****

Are Social Networking Sites A Threat to Nation's Security?

Man is a social animal and is naturally communicative. And we find this nature especially pronounced in a country like India. Indians are generally outspoken, ready to share and care. For this reason, not surprisingly, the social networking sites have always been a big hit in India, possibly growing at a faster pace than anywhere else in the world. Along with its popularity, the social networking medium also runs a high security risk for the user, as no messaging service can be stated to be 100% safe, secure and impenetrable. A service considered secure today could prove to be vulnerable tomorrow. Technology professionals are constantly casting aspersions on the security mechanism available, and are never confident about the fool-proof security strength of any technology.

WhatsApp, in its official website says, "*confidentiality and security are laid down in our DNA".* It adds that from the very first day it helps "*you stay in touch with your friends, share vital information during a disaster, reunite divorced families….share personal moments …we have built-in encryption*". It claims that the photos, videos, calls and documents shared over WhatsApp are protected against unauthorised access. It adds that it does not store the messages on its servers. But the flip side is that this very

assurance raises the concern of governments and investigators, engaged in solving and arresting cyber-crime and combating cyber terrorism.

There are interesting debates about lack of security in social networking sites, especially WhatsApp. In fact, there is a lurking fear as to whether one can eavesdrop on WhatsApp calls (i.e. intercepted and accessed) even though WhatsApp assures that the chats and calls are end-to-end encrypted. This assurance raises the comfort level of WhatsApp users in the sense that even if anyone tries to intercept messages using stealth technology, he would not be able to read (i.e. understand) the message. In technical parlance, it means that any chat message in WhatsApp travels in an encrypted mode, i.e. not in plain text. It can be decoded and understood only with the help of a specific decryption methodology only. The comfort one gets from this assurance is that even if anyone tries to intercept using technology, he would not be able to read (i.e. understand) the message.

On the flip side, however, this privacy of messages (which cannot be intercepted by anyone) can be a major threat to the security of a country. Often, there is criticism that security is breached as terrorists and anti-nationals exploit these private networking media to exchange security-threatening messages and instructions among themselves. Fortunately, there are software tools that can be used for mobile data recovery. These tools can also access WhatsApp data including stored text and pictures, even if they have been 'deleted'.

Of late, there have been many other messenger services emerging, to compete with WhatsApp, such as Telegram, which is gaining popularity. Telegram initially came up with the unique feature of self-deleting the message in the recipient's device too, within a few seconds after the message is sent and received at the other end. Recently, WhatsApp too added this facility of 'delete' or 'revoke' *after* the message has been sent. Although it is touted as a useful tool, it is an added nightmare for cyber-crime investigators because the evidence of messages exchanged between criminals and terrorists could then be destroyed.

And so, the debate continues on the question: "Which is supreme – the priority of the nation's security and sovereignty, OR individual data privacy"? The judiciary has repeatedly held that the nation's security is always supreme and of paramount importance, compared to individual privacy and data security. With the Data Privacy Act being discussed for immediate introduction, one hopes that the legislative provisions will be in place, removing ambiguity in the interpretation of what individual privacy is, and what national security and sovereignty is. India, as a nation in its fast-paced progress in the digital world, anxiously awaits.

By V Rajendran, Editor
Source : November 2017 issue of PreSense

*****

Bitcoins – Demystified

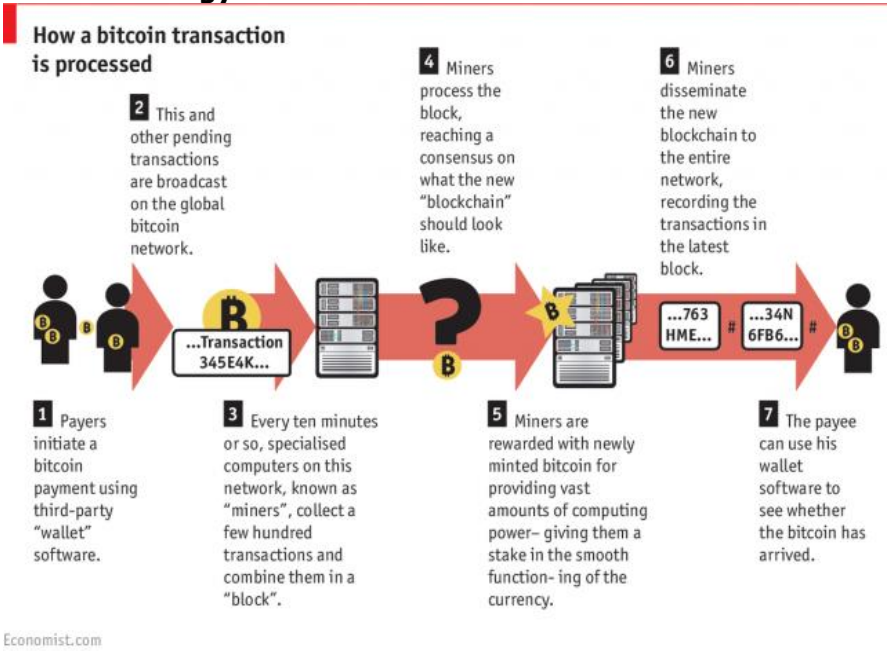
Currency, as an enabler to trade and payments, is as old as commerce, dating back to the earliest of civilisations. Every nation has its own currency. In international trade however, the medium of settlement for payments and commerce is often through the stronger currency or as per the agreement between the parties. The world is now witnessing a new form of currency, viz. cryptocurrency. It can be loosely equated to digital currency, although it is not exactly synonymous. In the organised and regulated market, there is always a systemic representation of the digital form of currency (as opposed to physical currency). In any economy, besides the physical currency notes in circulation, substantial exchange is also done through banking transactions i.e. in digital format, which represent a major part of the nation's economy. From this perspective, cryptocurrency does not represent the quantifiable, measurable and physical figure.

What is Bitcoin?

Bitcoin is a digital asset, and a payment system owned by nobody, regulated by none, and expressed as an open computer source software. It is accepted as a means of payment by a particular group of people. It was reportedly invented in 2009 by a Russian named Santoshi Nakamoto, whose biography is mysterious and not much is known about him (or maybe a group of men by that name, who could be the founders) for reasons better known to him/them. While introducing the concept of Bitcoin, the unknown person or people also introduced the first database for the technology called Blockchain, to enable payment through Bitcoin.

Every currency has a physical form – paper or a metal coin or both. In this cryptocurrency, it is just the computer system software i.e. the cryptographic source code that 'shows' the balance or 'evidences' the currency balance. Bitcoin is a cryptographically secure medium of financial exchange and not a 'fraud' though it comes under 'unregulated' medium. Bitcoin is basically 'digital' without a physical form. No doubt, in these days of e-commerce and online funds remittances, lots of financial transactions are in digital format.

The Technology Behind Bitcoin



Bitcoin functions in blockchain technology. Blockchain is a public distributed ledger verified by network nodes and authenticated through the computer source code in the app provided. It is an open source software, with no person, company or country owning this network, just as no one owns the Internet. In this system, users transact directly with the other end, without an intermediary like a bank or a credit card company or a clearing house. Since this is a computer based cryptographic technology, it has become easier in the modern day digital banking era, for banking transactions. Some private banks in India are reportedly transacting through blockchain already (although the regulator, the Reserve Bank of India, i.e. RBI, is yet to officially recognise or monitor this method of payment).

To open a Bitcoin account (or any cryptocurrency), you have to log in to their website, have a username created along with a password, and then have the initial money transferred from your e-wallet like PayTM. Alternatively, you can give this account

number from the ledger, to your clients and request them to pay to this account in this exchange itself, thereby converting your USD or INR invoice to this exchange-currency. You can later view in this ledger and trade in this exchange further, depending on that particular day's rate value, and, to be precise, the rate value at that particular time.

Bitcoin is not a monopoly. Although it was the number one cryptocurrency, other such currencies also functioning on the blockchain technology, are now catching on. Bitcoins, which once enjoyed more than 80% of the market share, has now reportedly come down to less than 40% market share. Ethereum, Ripple and Litecoin are accepted as alternative cryptocurrencies, rivalling Bitcoins.

The Regulatory Mechanism

Currently, cryptocurrency called by any name and of any origin, is not recognised in India by the financial regulator, RBI. Anyone trading in Bitcoins or other such cryptocurrencies would be doing so, completely at his own risk, playing in a field where there is no referee, no umpire, no intermediary and no rules and regulations. Even then, notwithstanding this uncertainty, the use of Bitcoins is on the rise and the volume of trade is increasing, especially among the high-stake financial players with an appetite for risk. It is said that although it is not recognised at present, the underlying technology behind cryptocurrencies will continue to exist. With a view to discourage the use of Bitcoins, the Finance Ministry has even labelled it as a worthless Ponzi Scheme.

The Global Scenario

Nations worldwide have not yet taken a clear stand on the use of cryptocurrencies. Understandably, it is feared that an unregulated and volatile system of payments and settlements has all the potential to destabilise any economy and derail the financial progress of the nation. Some nations have banned cryptocurrencies and called them illegal, while some have recognised it, while a few countries have not specifically banned it or called it illegal but recognised the underlying technology of

blockchains for transfer of funds. It is legal in countries like USA, Mexico, Canada, Brazil, Japan and Singapore, while countries like China and Russia have not recognised it as public currency.

High Value and Volatility

The currency is so volatile that its price fell from USD 19,000 on 16th December 2017 to a low of USD 12,000 on 30th December 2017. Perhaps it is this volatility that makes it interesting to many, and irresistible to those with a risk appetite.

In today's international trade, Bitcoin is the one with the highest value, a rate that is unimaginable, with even Google recognising it as a currency, and displaying its value in its normal searches. Today's Bitcoin market value is around INR. 6,30,000 (i.e. USD 9,800), which was once as low as INR 4,500 during 2010. Because of the high value, every Bitcoin is divisible to the 8th decimal place, which is the smallest unit of a Bitcoin.

Security Concerns

Besides the risk aspect, even on the security aspects, cryptocurrencies do not provide any comfort factor to the users. Already, some 175 million US dollars' worth of cryptocurrencies are reported to be 'stolen' as a result of hacking into the servers of just three exchanges so far. The exact figure remains unknown. With such a huge unregulated market, unmonitored transactions and intermediary-less opaque deals, where would one report these cyber-crimes? Since the value of cryptocurrencies is soaring, hackers consider it as easy-target-more-money than the conventional and normal electronic banking sites.

The Future

There are diverse opinions about the use, and the future of Bitcoins. Some people (frankly, very few) say that it is the future currency of the globe, though serious and learned economists are quite sceptical about the use of cryptocurrencies. The well-known American business magnate and philanthropist, Warren Buffet arguably among the most successful investors of the world, has

gone on record saying that cryptocurrencies have a bad ending and his firm was not interested in it. And recently, according to Forbes' latest list of billionaires, Satoshi Nakamoto, Bitcoin's mysterious inventor/s (where is he now?), is among the world's 50 richest people.

There are many corporates across the globe accepting or in the process of accepting Bitcoins as a medium of payment. In India too, as a first of its kind, some leading software giants have developed and are using the Blockchain technology, on which Bitcoins trading is done (and maybe other crypto-currencies too). Reliance Jio is now reportedly planning its own cryptocurrency to be called 'Jiocoin' and a young team of finance and software professionals is working to launch it soon.

If a few more companies join the bandwagon, it would be interesting to watch what stand our regulator, RBI will take to deal with the issue. As of now, the Finance Ministry has cautioned about the risk associated with these digital currencies and warned that they may become a tool for money laundering and other clandestine payments.

Here are some incredible but interesting titbits about Bitcoins:

- Just 1% of the Bitcoin community controls 99% of the Bitcoin wealth.
- Only around 900 people worldwide, own half of all Bitcoins.
- Ethereum, a popular cryptocurrency, saw an incredible increase of 3,888% in just 5 months i.e. from USD 5,000 to USD 199,400.
- Communication among the groups is mostly encoded and not easily accessible in the Internet.

To conclude**,** with everything becoming digitised (moving away from physical), it would be interesting to watch the progress of such cryptocurrencies. It would perhaps be like watching a performance from the gallery. Wisdom has to prevail upon the users to stay away from such unregulated, unmonitored market.

V Rajendran, Editor

Source: January 2018 issue of PreSense

***

A Genius of a Million Years, Stephen Hawking

The entire world wept when Professor Stephen William Hawking passed away on March 14th 2018 at the age of 76. He was the Director of Research at the Department of Applied Mathematics and Theoretical Physics and Founder of the Centre for Theoretical Cosmology at Cambridge, United Kingdom. It is interesting to know as to why the world should mourn the death of a scientist.

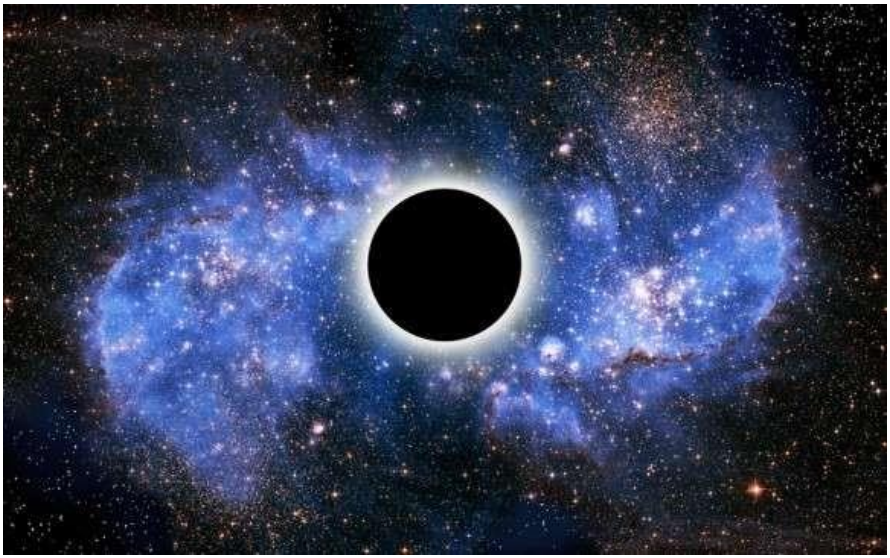
Understanding how our earth was created, how our solar system came into existence and how the universe itself was born, were questions of keen interest for mankind since the first man was born on earth about 4.2 million years ago.

Many things in the quest to understand the universe were not known until Professor Albert Einstein gave his powerful Theory of Relativity, which helped to understand the universe better. But when Professor Stephen William Hawking used the four tools of Relativity, Gravity, Quantum Mechanics and Thermodynamics to explain with amazing intelligence, almost all the mysteries about the origin of our entire universe and to some extent its possible

end are now understood beyond reasonable doubt. This is why Professor Stephen William Hawking is regarded a genius of a million years.

Hawking as a Genius Scientist

Professor Stephen Hawking worked on the basic laws which govern the universe. Hawking felt that it was necessary to unify Einstein's General Relativity Theory with Quantum Theory.



- To the surprise of the world, he went on to prove that black holes are not completely black, but that they emit radiation which we now call the 'Hawking' Radiation. By emitting such radiation, the black hole will eventually evaporate until it dies completely.

- Hawking mathematically proved that information cannot be lost inside a black hole but that in fact it is conserved.

- Hawking also proved that the universe has no direction, edge or boundary in imaginary time. This is like saying that there is no

north as a dimension or direction beyond the North Pole and the Earth.

Based on the above three contributions by Hawking, the world today considers him a genius of a million years, along with Einstein.

Hawking on the Future of Humanity

i) Safety of Life on Earth

Hawking used to ask, "In a world that is in chaos politically, socially and environmentally, how can the human race sustain another 100 years?". He elaborated, "I ask this question so that people can think about it, and to be aware of the dangers we now face." Hawking expressed concern that life on Earth was at risk from a sudden nuclear war, a genetically engineered virus, global warming, or other dangers humans have not yet thought of. Such a planet-wide disaster need not result in human extinction if the human race is able to colonise additional planets before the disaster. Hawking viewed spaceflight and the colonisation of space as necessary for the future of humanity.

ii) Aliens

Hawking stated that given the vastness of the universe, aliens are likely to exist, but that contact with them should be avoided. He warned that aliens might pillage the earth for resources. He said, "If aliens visit us, the outcome would be much as when Columbus landed in America, which did not turn out well for the Native Americans."

iii) Artificial Intelligence

Hawking warned that super intelligent Artificial Intelligence (AI) could be pivotal in steering the fate of the human race, stating that "the potential benefits are huge. Success in creating AI would be the biggest event in human history. It might also be the last unless we learn how to avoid the risks.

iv) Religion and Philosophy

He said that philosophical problems can be increasingly explained by science, particularly new scientific theories which "lead us to a new and very different picture of the universe and our place in it". He said that even if we assumed that God had decreed all the physical laws, God did not interfere to violate any of them. He was a vigorous supporter of the Many-Worlds Theory.

Personal Life of Hawking

Hawking had a very rare early onset of a slow-progressing form of motor neurone disease (also known as Amyotrophic Lateral Sclerosis, "ALS" or Lou Gehrig's Disease) that gradually led to paralysis, over the decades. Even after the loss of his speech, he was still able to communicate through a speech-generating device, initially through use of a hand-held switch, and eventually by using a single cheek muscle.

Uniqueness of Hawking

Stephen William Hawking was the distinguished Director of Research at the Centre for Theoretical Cosmology within the University of Cambridge. His books "A Brief History of Time" and "Theory of Everything" are extremely popular and more than a million copies of the former title were sold.

Hawking's dates of birth and death both hold special significance as he was born on the 300th death anniversary of Galileo and he died on 139th birth anniversary of Einstein.

Hawking's equation:

$$S = \frac{\pi A k c^3}{2 h G}$$

Key

S entropy
h the Planck constant
G Newton's constant
A area of event horizon
c speed of light
k Boltzmann's constant

Rare Honours Won by Hawking

Great Britain honoured him with its highest award, Commander of the British Empire. In a very rare gesture, former US President Barack Obama, awarded Hawking

The Presidential Medal of Freedom, which is the highest civilian award of America. This Award was presented for guiding humanity in a path-breaking manner using the highest order of science and ingenuity. Hawking is also in the elite group of the 100 Greatest Britons ever lived, according to a BBC-conducted poll.

Hawking's Last Wish

Hawking had often said, "We have this one life to appreciate the grand design of the universe, and for that, I am extremely grateful." Hawking wished that the Black Hole Equation which he formulated, be written on his tomb (*See image on right*).

By Prof. R Jagannathan, Editorial Advisor
Soutce: March 2018 issue of PreSense

***

Blockchain Technology

Blockchain technology is prophesied to change the world, portended to rock the banking industry and revolutionise its basic structure, just as the internet did, a few decades ago, in changing the way the world communicates. Blockchain technology is expected to change the way the world will transact business.

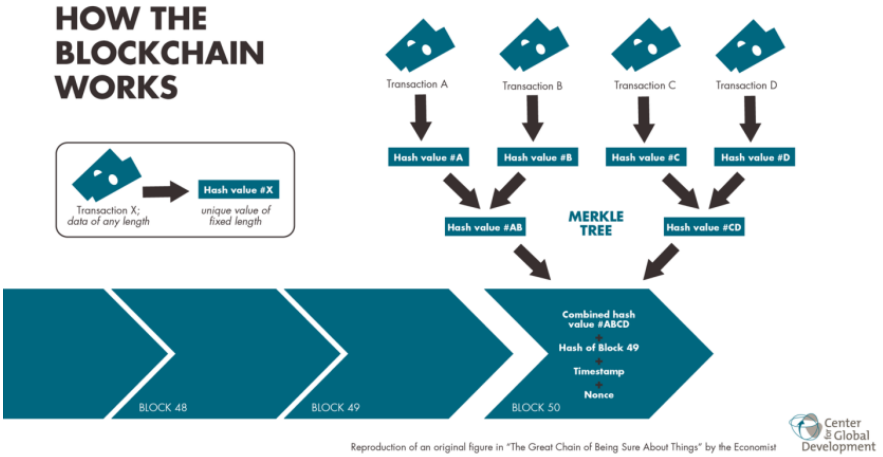
Blockchain technology is defined as a digitised and decentralised public ledger of all cryptocurrency transactions. For a quick re-cap on bitcoin, it is a virtual currency accepted in modes of payment and currencies of exchanges in a limited group within which it is traded, at the market determined rate, which is highly volatile. At today's prevailing rate, bitcoin is valued at around Rs.5 lakh (Rs.500,000) per coin (unit). Bitcoin is volatile, unpredictable, uncontrolled and completely unregulated as it has not yet come under any particular nation's regulatory mechanism. Some countries have not even recognised bitcoins as a currency. India too has not, so far. (Your emagazine, PreSense carried a detailed story on Bitcoin in its January 2018 issue).

Understanding Blockchain Technology

Blockchain technology is the system on which virtual currencies like bitcoins and ethereums (development platforms) actually sit. A blockchain can be compared to the Operating System (like MS Windows or Mac etc) of a computer, on which applications like Browser and Office Suite are loaded, and function. A blockchain is like a public ledger in which the participants maintain accounts in the form of virtual currency or crypto-currency called bitcoins or ethereums.

Blockchain was originally developed as an accounting method exclusively for the bitcoin currency, but in a short span of a few years, this technology has progressed greater in its development

as compared to that of bitcoins, for which it was conceptualised. Blockchains have been growing at such a pace that observers say, it is going to re-write history in the global e-commerce arena. Since a blockchain is maintained in a digitised and decentralised format, it is deemed to be tamper evident, and maintained in an immutable manner.



It reduces the friction among the various participants in commerce, traces the product and keeps track of it at every stage as a block. For instance, when you buy a car, many parties and lots of contractual obligations are involved in several stages, like the manufacturer's ledger (books) with the progress recorded therein, the dealer or the wholesaler's ledgers, the financier's books (if any), the registration authorities and then the ultimate consumer's ledgers. In a blockchain, the manufacturer, as a participant, marks the models being manufactured and other details.

The dealer thus gets to know the number of vehicles available, with complete details. The regulatory government authorities mark the same with details for registration and numbering purposes and the financier or the leasing company marks the same as part of the

contractual obligation between the lessor and the lessee. The ultimate consumer or user has all these details by the time the vehicle is delivered to him.

From the above example, it is evident that blockchain stores the transaction data in blocks in such a way that each block is linked to the next and the entire process is completely transparent and tamperproof. Each block leads to the next and the sequence is maintained, preventing any *ad hoc* insertion or alteration. Each participant in the chain is like a node in a network, accessing through a hash algorithm in a secure manner with a user ID and password, with a copy of the blockchain downloaded automatically.

Application of Blockchain Technology

In commerce, ledgers are conventionally and typically maintained at every entity, ie. at every participant's level, whereas in a blockchain there is a common ledger through which the transaction flows across all the stake holders, enabling all the participants to view the entire process-flow. It is distinct from a database and hence can be linked to any database including banking. Blockchain can be compared to a SWIFT (Society for Worldwide Interbank Financial Telecommunication) transaction that enables trade payment among all member banks, ensuring security of communication. It is generally a stand-alone package that should be systemically or manually integrated with the Core Banking Solution of the bank.

In a blockchain, the transaction is traced across the various members and is by itself a distinct technology and database. It is therefore, not a replacement of databases, or a messaging technology, but treated only as a supplement. In other words, blockchain may eventually replace the banking services or at least reduce its dependence to some extent, with many transactions going across through this technology as inter-party, in an e-

commerce transaction, and the various contracts, various sets of bi-polar or two-party contracting parties at every stage getting replaced with a single smart contract in this block.

There are various parties to a blockchain. The user is a participant who conducts the transaction and is not directly concerned with the technology (like a customer of a bank is unmindful of the technology in the bank). The regulator has special permission to oversee the transaction and does not conduct any transaction, whereas the network operator has permissions to create, define and monitor the network (like the Database Administrator in a Core Banking Data Centre). Programmers and developers enable traditional data transfer from existing databases of legacy firms and participants to the block through an electronic data interface, data exchange and other data transfer modalities.

Blockchain technology is believed to be an efficient tool especially in the area of supply chains, allowing new companies even in a private blockchain and thus leveraging start-ups too. Larger

companies can do business with smaller firms with reduced costs in market identification, legalities of contacts, supply chain management etc. Not just in supply chain, blockchain is expected to have a greater impact on financial services, government, manufacturing services as well especially towards effective and efficient use of intermediaries.

Status of Blockchain Technology in India

In India, a couple of months ago, in an interbank interactive survey, it transpired that 13% of the banks were already in production implementation of blockchain technology, while 30% were in the Proof of Concept stage with blockchain provider firms; 44% in the stage of formulating a strategy and evaluation, and the remaining 13% were 'looking into the technology'.

This is perhaps an indicator that the blockchain technology has come to stay in India. BankChain is reported be India's first Blockchain exploration consortium announced by the public sector giant, State Bank of India in February 2017, launched with more than 30 banks and NBFCs, National Payment Corporation of India, several foreign and private sector banks and a few public sector banks as members, in partnership with Microsoft, IBM, Data Security Council of India for expertise in their respective areas.

by V Rajendran, Editor
Source: May 2018 issue of PreSense

*****

Data Privacy Act – How it Will Impact Internet users?

Last week, the European Union (EU) came out with its General Data Protection Regulations popularly known as GDPR, implementing it with effect from 25 May 2018 in all the EU nations. This implementation will have a huge impact on all the nations, industries and of entities having trade and other obligations with Great Britain and other EU nations. On the first day of implementation of GDPR itself, it was reported that Facebook and Google had to face lawsuits costing millions of dollars for alleged data breaches and violations of data privacy.

What is GDPR?

GDPR is a regulation that gives control to citizens and residents over their personal data, with clear stipulations on the processing of personally identifiable information of data. It ensures that data is not available publicly without explicit consent, and it is stored and handled with utmost privacy settings within accepted lawful methodologies. GDPR is now implemented after a transition period of more than two years since its adoption in April 2016. These regulations mainly apply to any information relating to an individual, in private, professional or public life and can include such information as a name, a home address, a photo, an email address, bank details, posts on social networking sites, or medical information. For this reason, the implementation of GDPR is a significant landmark.

With the passing of CISA (Cyber Security Information Sharing Act) in USA effective from Dec 2015 and similar legislations in many other nations including GDPR in the EU, it is now time for India to come out with her own Data Privacy regulations. Perhaps as a first step and in the right direction too, the Government is setting up a committee to go into the issue of regulating the social networking sites including the right to express freely, e-publish news and fake news and other forms of views, opinions and what is camouflaged as 'news'.

Monitoring of Social Media

It is also reported that the government might put in place a huge data analytical software tool to monitor the data that is freely exchanged in social networking sites. Although the government informed that it proposed to deploy such software tools, one is not sure if these tools are already deployed by any firm or corporate or even individuals for profiling, spying, analysing, or even investigating for crimes, including pre-recruitment checks by corporate Human Resources officials, familial verifications for matrimonial alliances etc. When a Data Privacy Act comes into effect, perhaps the government will get an official status to monitor such deployment or usage of such tools for monitoring and regulating data, even in the Internet. The government should anyway, have some control on the way data and information is currently freely handled and transmitted across the net, especially from a national security perspective. Many judicial decisions have underlined the fact that freedom of expression is not an unfettered one and that there can be reasonable restrictions on the same.

The Data Privacy Act is a landmark decision waiting to happen, especially in the background of increasingly notorious acts of fake and mischievously instigating news, and malice to people based on stolen information from private social platforms and the social media.

By V Rajendran, Editor
Source: May 2018 issue of PreSense

*****

Wearable Devices

Of late, the mobile handset, ubiquitous and more popular than the plain cell phone because of its additional features, has become essential for almost every person. Except where its use is restricted for security or courtesy reasons, the mobile handset is carried by every person and often extravagantly and extraneously flaunted as a status symbol, depending on the model, unique features and the cost of the handset.

These devices started off with the humble 'pager', which was the first *avatar* of the messaging service. Then came the cordless phone, as an extension to the landline phone, before the advent of the omnipresent device called the cell phone. Technologists argue that within the next few years, cell phones will give way to wearable devices with a technology that can be worn on the human body. It would be small, almost the size of a wristwatch or even a ring. Companies competing with one another, are coming out with innovations that feature devices with higher capabilities in miniscule sizes. At seminars and conferences, we get to know of such evolving technology and models from big brands like Apple iWatch and Google Glass and even smaller companies too.

The technology used in this type of devices includes Bluetooth, Wi-Fi, sensor and transmission techniques, to enable such capabilities as reading the pulse, the blood pressure and other features of a human body. One of the common uses of a wearable device would be tracking a user's vital signs or data related to health, fitness or even emotions exhibited by the person's physical features. Depending on the technology and features of the device, the cost could vary from low-end to high-end.

Some believe that these devices could replace the cell phone and the credit/debit cards. The wearer of this gadget, using the Bluetooth technology, would be able to attend to phone calls, gain access to rooms and halls, use it as a credit/debit card to pay and if the high cost raises the blood pressure, the blood pressure reading can be checked immediately too! Then, of course, orders for suitable medicines could be placed through an online purchase, or a cab could be booked through the device to leave the place for home or the hospital! If the health parameters show alarm, messages could be sent to the next of kin, or medical advice could be sought immediately, using this device.

On the flip side however, we know that the moment we started using a cell phone and other devices using GPS and Wi-Fi or any other form of connectivity, we lost much of our privacy. And now with these progressive devices, we are bound to lose more of our privacy like compromising even on our confidential information like critical health records and health parameters.

But then, that is what technology is all about – risking the threats of disruption and invasion as it becomes an essential and indispensable part of our lives.

by V Rajendran, Editor
Source : Sep 2018 issue of PreSense

*****

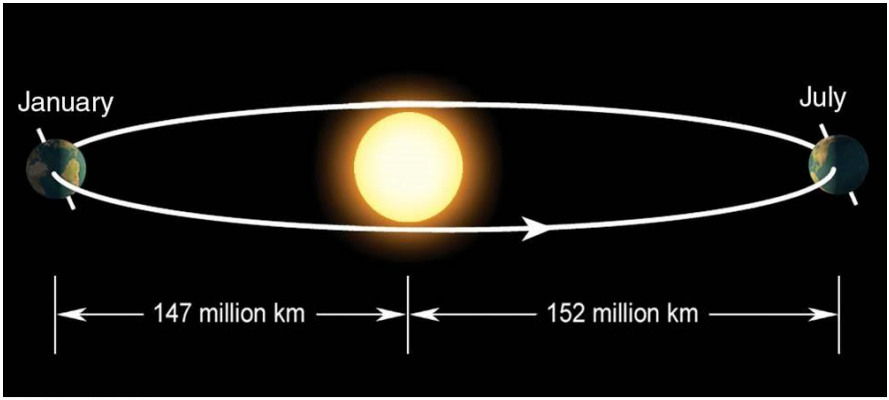
Our Very Own and Wonderful Sun

Whenever I look at the stars in the night sky or the Sun in the day sky, I realise how lucky we are to live on this planet and how insignificant we are in the realms of our solar system. When I walk on the street or see a tree, a pond, a river or a mountain, I realise the wonder and preciousness of our Earth, and how our Sun enabled all these wonders to exist. It is therefore no surprise why the Sun adorns a prominent place in the spiritual, religious, cultural and daily lives of all of us. Let us therefore get to know our life-giver and supporter, our very own Sun, better.

Birth of the Sun

Isolated hydrogen atoms in the free space of the galaxy, separated by distances of a few million kilometres (km), attract each other and over a prolonged period of time, start to form a lump. This

lump attracts more hydrogen atoms from the space and grows bigger. This process continues over a few hundred million years until the mass of the lump becomes incredibly big. The lump then starts shrinking inward in what is called a gravitational collapse. In this gravitational collapse which is a compression, heat is generated, leading to expansion. At one point, the shrinking due to gravitational collapse and the expansion due to the heat of compression, will balance each other. Now, we say a star of main sequence is born. This is how our Sun was born.



Interesting Facts about the Sun

When our Sun was born like this 4.6 billion years ago, a violent nuclear fusion reaction started at its core. It is energising our Sun even today. Our Sun has about 99.8 % of the mass of our solar system. If your weight is 100 kg on Earth, you will weigh 2800 kg on the surface of our Sun! The diameter of the Sun is such that we can place about 1 million Earths inside it!

Its core temperature is about 16 million ° C and its surface temperature is about 5500°C. Since it is an unsafeguarded nuclear reactor, all radioactive elements from helium to iron, are thrown out of the Sun, in all directions, on a 24x7x365 basis. We call these emissions solar winds and solar flares. The solar wind is a stream of energised, charged particles, primarily electrons and protons, flowing outward from the Sun, through the solar system at speeds as high as 900 km/s and at a temperature of about 1 million°C.

In addition to this, there are Coronal Mass Ejections (CME) in which the Sun, on an average, throws out fine radioactive particles of about 5 million kilogrammes every second with an average speed of 489 km/s.

So, the beautiful Sun that we see every day, is really a dangerously and violent nuclear reactor of diameter about 1.5 million km. Light takes about 8 minutes to travel from the Sun to Earth. It is interesting that the same light would have taken about a million years to travel from the core to the surface of the Sun. How strange is this Sun?

How Old is Our Sun and How Will it Die?

Our Sun is now a middle-aged star. It has enough hydrogen to sustain the nuclear fusion for another 5 billion years approximately. When its hydrogen content at the core is insufficient for the nuclear synthesis of helium, its effective life is over. It will then start expanding.

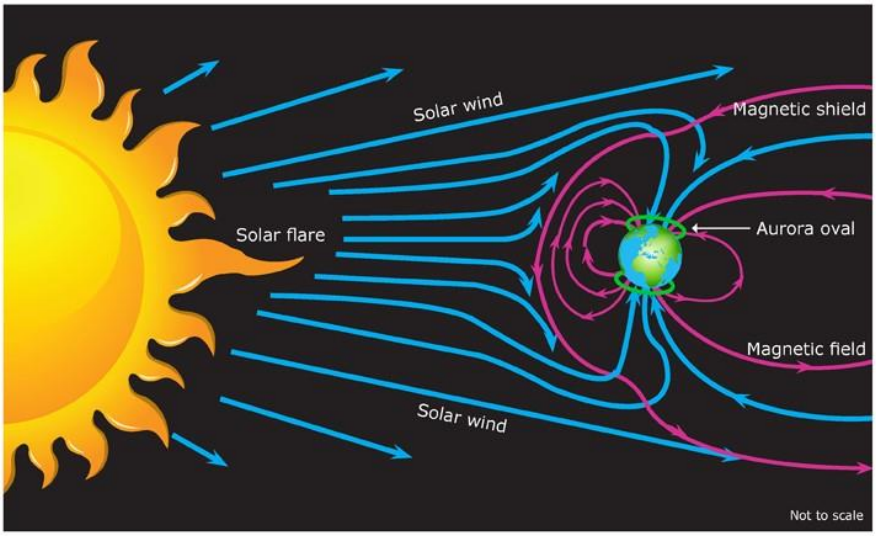
The expansion will go even beyond Pluto, engulfing all the planets, including our mother Earth. All life forms on Earth would be extinguished well before the expansion itself. When the sun expands like this, it will look red and huge and hence, it will be called a "red giant". When it becomes a red giant, at one point, it will shake itself violently shedding much of its own mass and in the process, it will become a very small white dwarf.

How Safe are We on Earth, from the Sun?

Earth's closest distance to the Sun is 147 million km and its farthest distance from the Sun is 152 million km. Had Earth been at a distance 10% closer than the present closest distance, then the noon temperature on Earth would be around 400 °C and life would not have been possible on Earth. On the other hand, had Earth been at a distance 10% farther away from the present farthest distance, then Earth's night temperature would have been around -200 °C and again, life would not have been possible on Earth.

The ionised particles thrown out by the Sun in the direction of Earth being in millions, all life forms on Earth would have been wiped out several million years ago itself. But life on Earth has survived due to the magnetic field of Earth. All the ionising particles coming from the Sun and the cosmos are deflected by Earth's magnetic field to land near the poles making other areas of Earth safe for life. This is evident from the picture released by the University of Waikato.

Conclusion



Our Earth is going around our central star – the Sun, which is a very violent un-safeguarded nuclear reactor. Fortunately, Earth's magnetic field saves us from the Sun's ionising radiations. Similarly, the distance of Earth from the Sun is so framed up in nature that life can sustain itself on Earth.

When nature has very delicately permitted and sustained life on this planet, must we pollute and degrade it? We must strive to live in peace, ignoring our differences of opinions, so that all of all us

can appreciate the concept of life in this solar system and enjoy the life that we are blessed with.

by Prof. R Jagannathan, Editorial Advisor
Source : Oct 2018 issue of PreSense

*****

Energy from Toilet Waste – Bringing Power to India

A recent news report confirmed that the Indian Rupee recovered sharply against the US Dollar, following a crash in the international crude oil prices. This respite is attributed to the 6-month waiver granted by USA to India on Iran sanctions. One must wait and watch the situation after the 6-month waiver expires and India must cease all imports from Iran, to adhere to USA's diktat. India has been one of the largest importers of oil from Iran. Such is the extent of India's dependence on imported oil for its domestic energy consumption needs.

Energy is an essential commodity in our lives for use in domestic and public lighting, running of essential machinery, transportation, travelling, in agriculture, manufacturing and service industries. Currently, India is dependent on imported oil to meet its energy requirements and the volatility of fuel prices, and unstable political and economic situations around the world, is not making it easy for India to ensure stable and affordable power resources. In this backdrop of bleakness and uncertainty, it is imperative that India looks to alternative means and strategies to ensure it does not plunge into darkness and to a grinding economic halt for want of sufficient power for its people.

India's focus for the power sector should be three-fold:

- Energy security – providing affordable, accessible energy to meet the growing demand.
- Energy independence - reducing the dependence on foreign resources or fossil fuel, and generating our own renewable resources to meet the growing needs. Fossil fuel is from coal, petroleum, diesel and natural gas.
- Reduction of carbon emission by cutting down on fossil fuel consumption and generating green power. This is possible by migrating to renewable energy resources, viz solar, wind, nuclear, biogas and hydrogen.

Current Power Situation in India

India is dependent on fossil fuel today for 75% of its total energy consumption. It is feared that the supply of fossil fuel would be depleted in another 20-30 years' time. The situation of fossil fuel dependency is somewhat similar the world over but every country has its own energy resource mix policy. For example, developed and cash-rich countries with advanced economies preserve their available indigenous energy resources for future, and are able to afford to buy energy resources from abroad for their present requirement.

For India, the way forward to resolve this energy crisis is to develop an effective technology to tap renewable energy resources. Today, only 5% of the country's energy consumption is from renewable energy resources.

Currently, India's energy consumption totalling 343,000MW (megawatt) (200,000MW in 2005, and projected to reach 450,000MW by 2030) is met from:

- fossil (coal, gas, diesel) – 220,000MW (energy efficiency of 60-75%)
- solar, biofuel, wind – 69,000MW (energy efficiency 35%)
- hydro – 45,000MW (energy efficiency 40%)
- nuclear – 7,000MW (energy efficiency 95%)

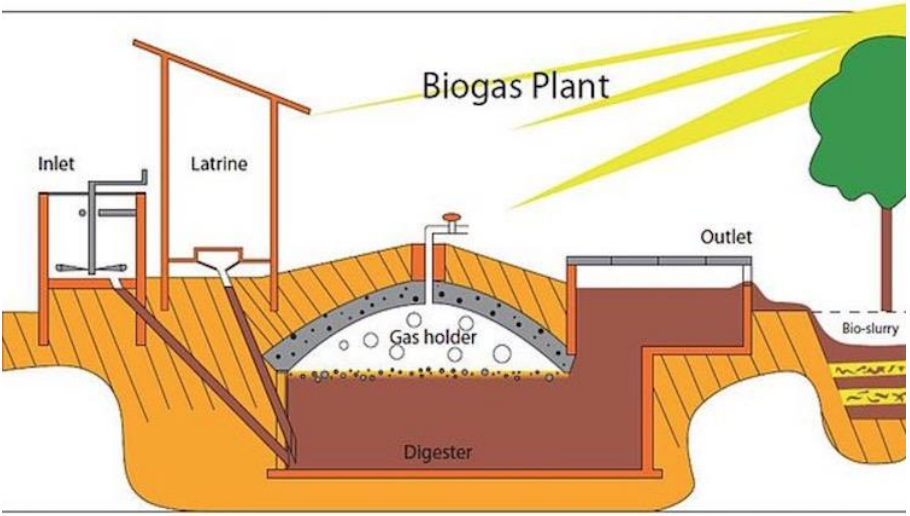
(Energy efficiency is the percentage of actual utilisation of energy from the supply available, excluding waste such as distribution leaks and pilferages.)

Interestingly, 1,000 MW of the total nuclear energy resource is from Tamil Nadu (Kudankulam and Kalpakkam projects).

The country sources renewable energy from wind (32,000 MW, of which 8,000 MW is from Tamil Nadu, especially Kanyakumari District, which supplies 5,000MW), solar (10,000 MW), biomass (8,000 MW), small hydro projects (4,500 MW) and municipal waste (1,000 MW). While

Energy Generation from Toilet

The ideal renewable energy source to be tapped, especially at the grass root level of villages, to bring India to an energy-sufficient level is municipal waste. Municipal waste is toilet waste. If toilet



waste is collected through a centralised drainage system in every village or locality, this can be a valuable, sustainable and economical source of energy to light up every house and meet much of the local energy requirements. Toilets in villages, including those constructed under the *Swachh Bharat Abhiyan* (Clean India Mission) are currently constructed as individual pits. These pits can also pose a health threat by contaminating groundwater and its TDS (total dissolved solids). If these pits are connected to a centralised biodigester plant and the waste treated, it would provide a source of energy and revenue for the villages.

The *panchayat* of an average village, with a population of 2500, has the capacity to generate 50-100 kW (kilowatt) from a municipal waste power generation project. Similarly, an urban municipality can generate 1MW, and an urban corporation can generate 5-10MW. Tamil Nadu State for example, has 153 municipalities and 14 corporations. The investment for generation

of 1MW energy from municipal waste is estimated at Rs.20-30 million.

Thirty-one educational institutions and industrial entities in Tamil Nadu have successfully implemented the municipal waste energy project which generates around 1392 kW in total. Two of the initial projects implemented are in Tamil Nadu – one at Sastra University which generates 72kW, and the other at Periyar PURA at Periyar Maniammai University which generates 60kW power.

These projects in Tamil Nadu were inaugurated by late Dr A.P.J Abdul Kalam (11th President of India) in 2009. With the implementation of this project, the universities are able to meet their captive energy requirements from the energy generated through the project. Two industrial entities in Tamil Nadu are generating 200kW each.

Unfortunately, the concept has not yet been successfully implemented at the village level because of the lack of coordination among the people required to be involved, viz. the Government (both State and Central), institutions, village *panchayats*, research departments and corporates.

The participation of corporates through their CSR (Corporate Social Responsibility) plans is critical here. The cost of the project is estimated at Rs.25 million which includes installation of centralisation drainage of toilets – Rs.10 million, central bio-digester plant – Rs.5 million, accessories – Rs.10 million.

Economics of Municipal Waste Energy Project

The process involved in the municipal waste energy project is as follows:

- When a village having 1,000 houses with toilets implements the project, 100 kWh energy can be generated per hour per village.
- At an average of 12 hours of generation per day, it generates 1200 kWh energy per day.

- By installing solar beams for solar energy generation, the captive energy requirement and public lighting can be met so that the municipal waste energy generated is available for sale to the Government grid @ Rs.3.47/- per KWh. The total revenue for the village per day will thus be Rs. 4164 and Rs. 124,920 per month or Rs. 1.5 million per annum.
- The RoI (Return on Investment) is achieved in 5 years' time, and there will be surplus revenue generated thence, available to the village *panchayat* for spending on the village, instead of depending on government disbursed funds.
- There could be public-private participation of say, 25% by the village *panchayat* and 75% by social enterprises like the Government (subsidy), banks (loans) and corporates (grants through CSR).
- An alternative is for each corporate to adopt at least one village, investing a maximum of Rs.20-25 million, so that the 200,000 village *panchayats* can be adopted by corporates under their CSR commitment.
- This project will also provide employment to the youth of the village at the rate of at least five youngsters per project, as they will run and maintain the project and ancillary enterprises.

A critical pre-requisite for this project is segregation. Rainwater harvesting facility should be installed to direct rainwater to the local ponds and lakes. Rainwater harvesting in individual homes will take the rainwater to self-owned sumps and water tanks. Bathroom/kitchen waste must be segregated from toilet waste before treating them separately. Bathroom waste can be used for outdoor water requirements and toilet waste can be used for energy generation.

Unfortunately, there has been little coordination among the governments, institutions and corporates. In spite of successful technological researches accomplished by the Government research departments, these lie underutilised and not implemented.

As Shri V. Ponraj, former Scientific Advisor to late Dr Kalam reflected with regret, "India has islands/beads of success, but no

one is making a garland out of these successful researches." Shri Ponraj had been associated with Dr Kalam in evolving the Energy Independences Vision 2030, propagating and promoting the concept of generating sustainable energy from renewable resources at affordable cost. He sees immense scope in this project, as according to him, India has 200 million houses, out of which 40 million houses remain without electricity.

In 2014, Dr Kalam had proposed the municipal waste energy generation concept while presenting the PURA (Provision of Urban Amenities to Rural Areas) Scheme, conceptualised by him for providing economic opportunities outside of cities. He had also detailed it in his book, 'A Manifesto for Change'.

Interestingly, Shri Ponraj had also recommended adoption of the Municipal Waste Energy Project in the Shyama Prakash Mukherjee RURBAN Mission (SPMRM) of the Government of India, launched in February 2016. SPMRM envisages development of rural growth clusters in all the states and Union Territories of the country to trigger overall development, by providing economic activities, development of skills and local entrepreneurship and infrastructural amenities. So far, there is little positive response to this recommendation.

Initiating Small Steps Towards Rural Development

In 2017, Ponraj with his team of people, adopted 24 villages in the district of Cuddalore in Tamil Nadu and initiated Dr Kalam's PURA scheme, with the support of the Cuddalore District Administration and funding by the Tamil Sangam, USA. The mission is threefold:

1) providing safe drinking water, 2) segregating the drainage system, and 3) connecting the toilets for implementing the municipal waste energy generation. The scheme has completed the first phase of the mission and 40,000 litres of RO-treated drinking water is generated from the local sources for the villagers. 'ATMs' have been installed in the villages to provide drinking water @ Rs.3 per litre.

The successful implementation of the Municipal Waste Power Generation Project will help in creating a clean, green and carbon-neutral India. We all could then dream of a country that is truly and rightfully an "Incredible India".

by Susan Koshy, Editor-in-Chief,
with input from Shri V Ponraj,
Former Scientific Advisor
to late Dr A.P.J. Abdul Kalam
Source : Nov 2018 issue of PreSense

*****

When It's December, We Greet New Nobel Laureates!

On December 10th every year, the Nobel Prize winners for the year are awarded the most coveted prize on earth – the Nobel Medal and the Diploma – by the King of Sweden. This year, King Carl XVI Gustaf of Sweden will present the Nobel prizes to those who are being recognised for contributing to the greatest benefit of humankind in Physics, Chemistry, Physiology or Medicine, Literature and Peace.

The Nobel Prize was instituted by the last will and testament of the inventor of dynamite, Alfred Bernhard Nobel. The Nobel Awards and Prizes have been awarded since 1901. In his will dated November 27, 1895, Alfred Nobel had stated, "It is my express wish that when awarding the prizes, no consideration be given to nationality, but that the prize be awarded to the worthiest person." The Nobel prize winners are selected by an extraordinarily neutral and impartial process. No information of the selection process can be revealed for a 50-year period. Let us see the discoveries made by the scientists who will receive the award this year.

Nobel Awards and Prize for 2018

Nobel Award for Physics: **Arthur Ashkin** invented optical tweezers that can grab particles, atoms, viruses and other living cells with their laser beam fingers. A major breakthrough came in 1987 when Ashkin used the tweezers to capture living bacteria without harming them. He was able to study the biological systems. Optical tweezers are now widely used to investigate the machinery of life.

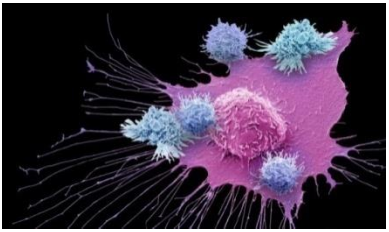
Gérard Mourou and **Donna Strickland** paved the way to the creation of the shortest and most intense laser pulses. Their revolutionary article was published in 1985 and it was the foundation of Strickland's doctoral thesis. Using an ingenious approach, they succeeded in creating ultrashort high-

intensity laser pulses. Its uses include millions of corrective eye surgeries (*see adjoining picture*) that are conducted every year using the sharpest of laser beams.

The innumerable areas of application of the discoveries of these scientists have not yet been completely explored. However, even now, these inventions allow us to rummage around in the microworld in the spirit of Alfred Nobel's will – for the greatest benefit of humankind. These three great scientists are awarded the 2018 Nobel Prize for Physics.

Nobel Award for Chemistry: This year's Nobel Laureates in Chemistry were inspired by the power of evolution and used the same principles – genetic change and selection – to develop proteins that solve mankind's chemical problems.

In 1993, Frances H. Arnold conducted the first directed evolution of enzymes, which are proteins. The enzymes developed by Frances Arnold are used in the manufacture of chemical substances that are more environmentally friendly, such as pharmaceuticals, and in the production of renewable fuels for a greener transport sector. In 1985, **George P. Smith** developed an elegant method known as phage display, where a bacteriophage – a virus that infects bacteria – can be used to evolve new proteins. Sir Gregory Winter used phage display for the directed evolution of antibodies, with the aim of producing new pharmaceuticals. The first pharmaceutical based on this method called adalimumab, was approved in 2002 and is used for rheumatoid arthritis, psoriasis and inflammatory bowel diseases. Since then, phage display has produced anti-bodies that can neutralise toxins, counteract auto-immune diseases and cure metastatic cancer.



Physiology/Medicine Nobel Prize: Cancer kills millions of people every year and it is one of humanity's greatest health challenges. By stimulating the inherent ability of our immune system to attack the tumour cells, this year's Nobel

Laureates have established an entirely new principle for cancer therapy.

James P. Allison studied a known protein that functions as a brake on the immune system. He realised the potential of releasing the brake and thereby unleashing our immune cells to attack the tumours. He then developed this concept into a new approach for treating patients for cancer.

Tasuku Honjo discovered a protein on immune cells and, after careful exploration of its function, eventually revealed that it also operates as a brake, but with a different mechanism of action. Therapies based on his discovery proved to be strikingly effective in the fight against cancer.

Allison and Honjo showed how different strategies for inhibiting the brakes on the immune system can be used in the treatment of cancer. The seminal discoveries by the two Laureates constitute a landmark in our fight against cancer.

Nobel Prize for Peace: This year's Nobel Peace Prize is firmly embedded in the criteria spelled out in Alfred Nobel's will. Denis Mukwege and Nadia Murad have both put their personal security at risk by courageously combating war crimes and seeking justice for the victims. They have thereby promoted the fraternity of nations through the application of principles of international law.

Nobel Prize for Literature: For the first time since 1949, the Secretive Jury that hands out the world's most prestigious Literary Nobel Prize, has announced that there will be no recipient for the Nobel Prize for Literature this year, but it will be given to two people in 2019.

Epilogue: This year 12 new laureates have been recognised for the Nobel Awards and Prizes for achievements that have contributed to the greatest benefit to humankind. Their work and discoveries range from cancer therapy and laser physics to developing proteins that can solve humankind's chemical problems. The work of the 2018 Nobel Laureates also include combating war crimes, as well as integrating innovation with economic growth.

India is a country with the youth forming a majority of its population. It is the dream of every Indian to see a young Indian win the most coveted Nobel prize in the coming years.

by Dr R Jagannathan, Editorial Advisor
Source : Nov 2018 issue of PreSense

*****

Digital Signature – Demystified

Why do we sign a document? We do so to authenticate the contents of the document, so that people can rely on it as genuine. When you receive a letter from your friend, you know his handwriting, and you rely on it as authentic and irrefutable. Instead of a hand-written letter, if he types it out, or prints it out, he signs at the end of the letter to convey that he takes responsibility for the contents, thus adding authenticity to it. If you have a friend by the name 'Ram' and you receive an email from him, how do you know that the sender is your friend Ram? Anyone can create an email in any name. Suppose a fraudster creates an email in the name of 'ram' and adds a photo of your friend Ram at the bottom of the email to make you believe that the sender is indeed your friend Ram, then in such a case of electronic communication, how does one add authenticity?

The Three Pillars

In professional parlance, Confidentiality, Integrity, and Availability are stated to be the three pillars of data security. Some professionals add a fourth pillar to these with features like Non-repudiation, Authorisation, Accountability, Authentication etc. Integrity is the quality to convey that the document cannot be tampered with. Non-repudiation is the quality of non-denial *ie.* the sender should not be permitted to deny having sent it, nor the receiver be permitted to deny having received it. In a digital communication, the above attributes of security are fulfilled by a process called 'Digital Signature'. Yes, it is a process.

What is a Digital Signature?

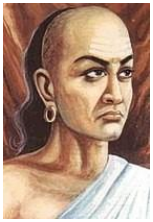
Digital Signature is not a signature at all. A human signature is not affixed. To put it simply, a digital signature does not contain our 'signature' in the common sense of the term and we do not 'sign' in it. A Digital Signature is a mathematical technique used to authenticate an electronic message or a digital document. It is the electronic or digital equivalent of a handwritten signature, a stamp or a seal, offering security, and safeguarding the communication or message from tampering and impersonation.

In the case of a digitally signed document, a trigger such as an SMS alert, pops up a message stating that there is a message for you. When it is clicked, it will ask for your user name and password. This process of opening the mail or communication (like NEFT or RTGS etc) is called digitally signing the document with a private key. One needs to use the designated computer system to open the document. In the absence of that particular computer system or chip card, anyone just using the registered login and password cannot open the digitally secured document. This is because that computer might not have the specific software which acts as the public key. The login and password form the private key. Both the public and private keys have to be used in combination to create an alphanumeric value called the hash value. This process is also called verification of signature by the Digital Signature Certifying Authority. A digitally signed document is different from a digitally secured or a password-protected document which asks only for the password to open it. Anyone who enters the password from any computer, can open the document.

The Digital Signature Certificate (DSC) is issued by one of the nine authorised DSC entities (like National Informatics Centre, IDRBT, eMudra, TCS, etc) in the form of a chip-card or a pen drive, containing basic details. When it is inserted in our computer system containing the basic software, then whenever we send an electronic document, and we type our user name and password (which is called the private key), this, together with the basic software in the device, generates a value, *ie*. our signature is certified by the authority in a process called the public-key and private-key infrastructure. The document travels in an encrypted manner from the sender to the receiver in such a way that anyone intervening, will NOT be able to read or understand. At the other end, the email receiver also applies his user name and password which, when authenticated, will open the mail. Thus, the confidentiality, integrity and non-repudiation are fulfilled.

What is Encryption?

Since the data (or message or email) travels in a public medium/public communication network, it should go in an encrypted manner. Encryption is the process of converting the message into such a format that no one, other than the sender and the authorised receiver, should be permitted to 'open' it to read and understand it.



Interestingly, the process of encryption of a message sent in a public medium was used in many ancient Indian epics like *Mahabharata*. Kautilya (Chanakya) in his much-acclaimed administrative treatise, "*Arthashastra*" said that any confidential message sent through a public messenger from one minister or ruler to another minister or ruler should always be encrypted.

Symmetric encryption is the process of encrypting and decrypting in the same manner. For example, if we want to convey the word 'ezine' it is encrypted as 'dyhmd'. This is simple encryption where every letter in the word 'ezine' is substituted by its preceding letter to make it incomprehensible. Digital Signature does NOT use this method of symmetric encryption. It uses asymmetric encryption, where the encryption and decryption follow different methodologies and only after deploying the software tool available with the receiver and the sender, can the message be encrypted or decrypted.

Bank Remittances

All the banks (the officials engaged in financial remittances like RTGS and NEFT among banks) in India use Digital Signature Certificates, issued by the Institute for Development and Research in Banking Technology (IDRBT), Hyderabad, which is the research wing of the Reserve Bank India (RBI). These are therefore always safe, secure and never intercepted or tampered with. Chartered Accountants and other professionals dealing with government taxation related documents use Digital Signatures for submission of documents to the government departments like Income Tax, Sales Tax etc.

Digital Signature certifying processes and its meaning, definition and application were originally dealt with in detail in the Information Technology Act 2000. Since that Act recognised only the method of private key and public key infrastructure as discussed above, the words 'Digital Signature' was later replaced with 'Electronic Signature' in the IT Amendment Act 2008, to make it technology-neutral. Any mechanism of biometric authentication and any other technology that fulfils the attributes of information security and its related qualities like asymmetric encryption *etc*, are now recognised as legal in India.

by V Rajendran, Editor
Source : Dec 2018 issue of PreSense

*****

TikTok – the New Hype in Multimedia Apps

What is TikTok? TikTok is a media app for creating and sharing short videos. It is gaining ever-increasing popularity especially in the Indian market. According to Wikipedia, it is owned by ByteDance, which is a Chinese internet technology company, and it was launched as Douyin in China in September 2016. ByteDance took just 200 days to develop this app. A year later, it was introduced in the overseas market as TikTok, and it got around 100 million users within a year. It is now stated to be available in over 150 nations in 75 languages. It is also said to have surpassed Facebook, YouTube and Instagram in subscriptions, and have become the world's most downloaded app in the iOS.

How to Use?

The TikTok app is downloadable from Play Store to the phone's operating system such as Android or Apple iOS. After its installation, one can login, using the Facebook or Google user ID, or by creating a new and independent user ID. Thereafter, one gains access to a list of popular videos, to which one can upload one's voiceover, or voice to sync with the video, or even add one's own video to give the effect that they are part of the original video. TikTok must be appreciated as part of innovative technology. Facebook is reportedly working on a similar app as TikTok, with comparable features, and standalone music and video sync capabilities like karaoke.

What is the Flip Side?

Technology users, especially the mobile app users, are flooded with memes. The WhatsApp is bombarded with memes – especially of celebrities, some of them in harmless tease, some in light humour and some others bordering on defamation, mud-slinging and character assassination of the celebrity. The police and the courts have to deliberate and discuss to determine whether the meme is a penal offence of character assassination or defamation, or just a harmless joke enjoyed as 'freedom of expression in a public domain'.

The memes that are created and posted are rated as successful or popular on the basis of the number of times they are re-tweeted, forwarded or shared, and the extent to which they have spread as viral in the internet. In the process, the celebrity or person whose picture or video is the subject of the meme, becomes popular or notorious, depending on the flavour of the meme. Some of the celebrities take them as offensive and resort to legal recourse, while many ignore them.

What is the Solution?

Faced with the serious threat that this app poses through its misuse, the Government of Tamil Nadu has decided to approach the Centre Government, seeking the ban of this app from the public domain. But would this move be the ultimate solution? While the right of the government seeking a ban on any app, or for that matter, any internet web page or website or contents, is legible and legal, and we do appreciate its judicious use of such right with due restraint, we have to look at the practical implications of such an action. Blocking and banning may be an immediate remedy, but would it pay in the long run? We are all aware that if a building site is demolished because it is an illegal construction erected in gross violation of local administrative guidelines, it takes at least a few months if not years for someone who, out of audacity, would want to construct a similar site in the same place. But in the case of a website, it takes barely a few minutes, not months or weeks,

to set up an app with a slight modification in the name, but with similar objectionable contents and intention.

What then is the solution? It is not the severity of laws that serves as a deterrent to crime, but the certainty of punishment. Governments have to work and act consistently and tirelessly, leaving no stones unturned, in its pursuit to regulate the internet and book offenders. The internet is aptly called an 'uncontrolled beast'. Any attempt to control such beasts, floating in the virtual world as apps and malware, should be welcome by netizens and not be criticised as curtailment of the freedom of expression. After all, what is entertaining to one, could be offensive to another. Ultimately, it is the adherence to the fundamental rules of netiquette, and cooperation with the law, that could help curtail the misuse of TikTok and its memes.

by V Rajendran, Editor
Source : Feb 2019 issue of PreSense

*****

Digital Disputes

From ***e-***commerce, ***e***mail, ***e-***banking and ***e-***payments to ***e-***verything, the buzz-word today is to prefix a word with "***e***-" and make it digital! The entire world is going digital. Naturally, we have to gear up for digital disputes too. If we buy goods physically from a shop in a nearby mall, we go there to discuss the issue and sometimes return the same or take remedial steps. If we buy goods online and the goods prove defective, what happens? Do we incur the expenses of re-packing and mailing it back, and then claim refund? In such a case, if the return or any other terms of the contract is disputed, where do we go? Even assuming we are not importing it and are buying it locally, under whose jurisdiction does the transaction fall? Interesting questions…..often debated and decided by courts too, based on the nature of transactions, type of goods, the legal remedy arising out of contravention and the Act under which the action is governed.

The strength and popularity of *e*-commerce lies in the statement that the biggest cab operator does not own a single taxi, the biggest caterer does not produce a single food item, the biggest real estate agent does not own a single building and so on. So perhaps, the biggest retailer does not stock a single provision or grocery item. All these are just technologically strong middlemen. Hence the disputes arising from these transactions too, are more technological or techno-legal to be precise, and less physical. Although the Information Technology Act 2000 recognises electronic records as valid evidences – a position which has almost stabilised for nearly two decades now – the legal status of *e*-commerce, especially for the small-time consumer, continues to be often debated. This consumer is often unsure about his options and whom he could approach in case of a dispute.

Basically, it is the terms of contract of sale that govern the transaction and naturally, the terms have to be read thoroughly. In practice however, especially when the terms of a contract or agreement run into pages, at the end of which is an "*I Agree*" button, we simply scroll down to the final page and click that button to proceed/continue. How many of us do actually read the entire document, and understand it?

A simple legal redress is that a contract is materialised when an offer is accepted by acceptance, and at the place where accepted. Hence to put it in simple words, an *e*-commerce transaction is completed as a contract and in case of a dispute, the buyer's place will have jurisdiction. This simple issue of a sale transaction can get complicated if the seller is abroad or the buyer's place itself is ambiguous *ie* a person residing abroad, ensuring delivery in an Indian city and making payment from a foreign bank and foreign branch.

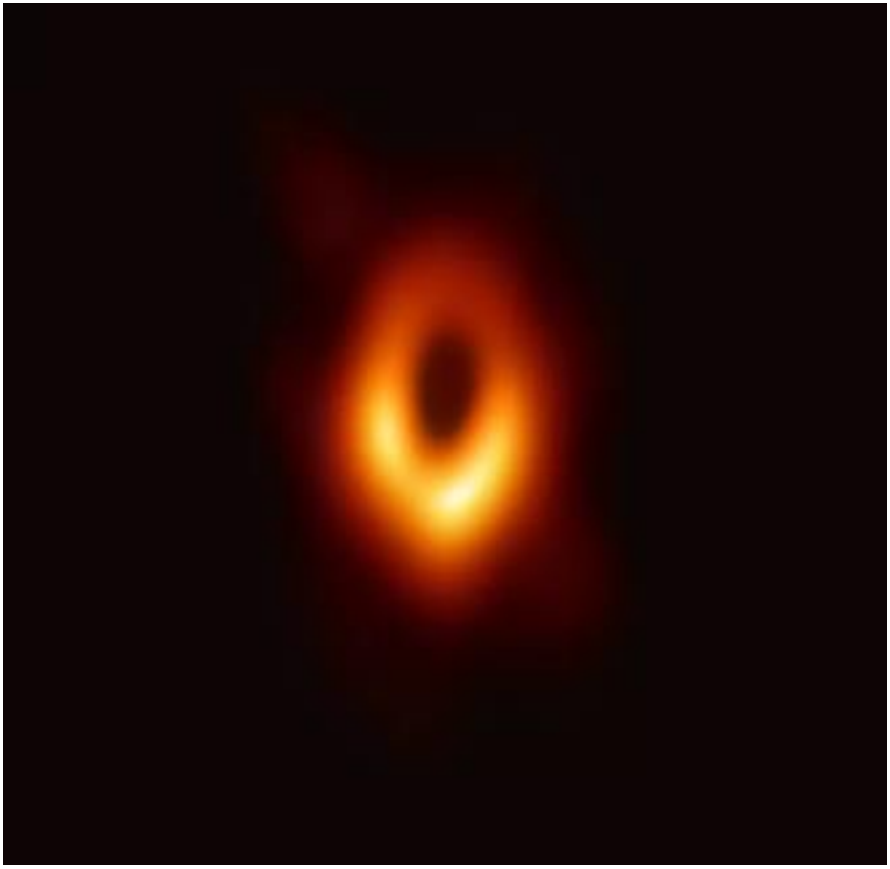
"*Caveat Emptor*" is a Latin phrase and an old adage to mean "*Let the buyer beware*". In other words, the buyer is to be cautious about the nature of the goods bought *ie* on an *'as is where is'* condition or something to that effect. Perhaps, in an *e*-commerce, it should be "buyer ***e***-beware" *ie* the buyer should ***e***lectronically or even ***e***xcessively beware of the terms of the trade.

by V Rajendran, Editor
Source : March 2019 issue of PreSense

*****

Black Hole – Finally Captured by Mankind!

Introduction



It is a moment of pride for all of us living on Planet Earth, as we advance in our understanding about black holes, to capture one of them in a photograph!

The name 'black hole' is a misnomer in the sense that it is not a hole in the sky but is a massive star, which captures/absorbs even light so that it looks like a black hole in the sky.

The black hole in the M87 Galaxy, which is about 55 million light years away, has been successfully photographed by mankind for the first time in history, after 20 years of persistent and intense efforts by international scientists. (*A light year is a unit of distance, used for measuring the astronomical distances in outer space. A light year is the distance travelled by light in one year. Light travels at a velocity of about 300,000 kilometre per second. It travels nearly 10 trillion kilometres in a year*).

Evolution: From a Hydrogen Atom to a Star to a White Dwarf to a Black Hole

Hydrogen Atom to a Star: The hydrogen atoms in the universe, by gravitational attraction, form groups, grow in size and become a bigger and heavier cluster. In about 10 million years, the cluster becomes a star. Our Sun, called a G-Type star, was formed in a similar way. Its life span is about 10 billion years and our Sun is now middle aged!

Star to a White Dwarf: In 1931, Indian Nobel Laureate Prof. Subramanyan Chandrasekhar established that a special type of stars called white dwarfs are formed and they can have a maximum mass of 1.4 solar masses, which is now called the Chandrasekar limit. (*Solar Mass is the mass of our Sun, and it is used as a unit of mass*). These heavy stars are very small but brilliantly bright!

White Dwarf to a Black Hole: When a white dwarf acquires more and more material and its mass exceeds 1.4 solar mass, it becomes a black hole. If any object falls into the event horizon of a black hole, it cannot return or come out. Even light cannot escape its gravitational pull. The event horizon is a region around a blackhole which is called the point-of-no-return, where any body (even light) entering that region cannot escape and it becomes part of the blackhole.

Why is Even Light Not Able to Escape from a Black Hole?

Imagine that you are throwing a stone upwards. The stone falls back down to the ground because the earth's gravity

attracts/draws it. The stone is not able to escape the earth's gravitation pull because the speed with which you have thrown it up is less than that of the downward pull. If you can throw the stone at a speed of 11.2 km per second, then the stone will have sufficient energy to escape the gravitational pull of earth once and for all. This speed is called the 'Escape Velocity' of Earth. The more massive the planet is, the greater its escape velocity. The escape velocity of some of the known space objects are as below:

S. No.	Body	Mass	Escape Velocity: Km per Second
1.	Our Moon	1/80th Earth's mass	2.4
2.	Earth	6 crore crore crore tonnes (6 billion trillion tonnes)	11.2
3.	Jupiter	318 times Earth's mass	60
4.	Our Sun	333,000 times Earth's mass	617

Thus, we find that the speed required to escape from the planet/star becomes greater as its mass increases. It is logical to conclude that for a certain mass of the star, the escape velocity will be the same as the speed of light. At that point, all matter, including radiation and light, once it goes near such a massive body, will fall into it. Even if an object or light goes so close such a massive body, into the region called 'point of no return' or the event horizon of such a massive star, it will be sucked into the star and such a massive body will simply look like a black hole in the sky. A black hole is a supermassive star.

How Could the Black Hole be Photographed Now?

The Event Horizon Telescope (EHT) is a consortium of more than 200 scientists who worked day and night for about two decades. It is truly an international endeavour. Funding over the years came from the U.S. National Science Foundation and many other organisations of countries around the world. The project has been scrutinising two black holes — the M87 behemoth, which harbours

about 6.5 billion times the mass of our sun, and our own Milky Way Galaxy's central black hole, known as Sagittarius A, having a mass of a mere 4.3 million solar masses. The scientists decided to track and photograph the M87 blackhole, since they thought it will be easier to resolve in spite of its long distance.

No single telescope on Earth can make that observation, so the EHT team had to get creative. The researchers linked up radio telescopes in Arizona, Spain, Mexico, Antarctica and other places around the world, forming a virtual radio telescope the size of Earth. This technique is called Very Large Base Line Interferometry (VLBLI). The EHT team used VLBI to capture the black hole's shadow against the light of the surrounding stars.

Conclusion

This photographing of a black hole is just the beginning. Other such holes, with different masses, spins, and orientations are potential targets for future observation. As further technological refinements are made to the EHT's capabilities, we stand a good chance of producing even finer dissections of the outer anatomy of these absurd, beautiful, and terrifying places, throwing more light about our Universe. The night sky we are familiar with, is truly deceptively calm and charming!

by Dr R Jagannathan, Editorial Adviser
Source : April 2019 issue of PreSense

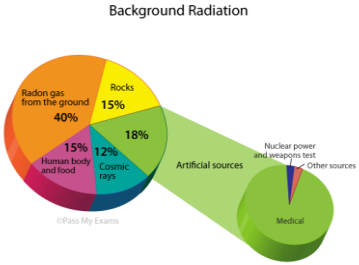
*****

Nuclear Radiation and Nuclear Waste Management

Background Radiation

Mankind is exposed 24X7daily to nuclear radiation, coming from three sources. One source is the radiation coming from the centre of Earth continuously at different intensity levels at different places - but it covers all places. The second source is radiation from the 'cosmos' - the space – in all directions, again 24X7. Most of the cosmic radiation is deflected towards the north and south poles of Earth, by Earth's magnetic field. The third source is our own atmosphere which emits radiation from the radon gas, generated by the Earth's crust.

The total radiation from all these above three sources put together is called 'Background Radiation' of Earth at any given place on Earth. None of us can escape from this background radiation. All of us, generation after generation, have been receiving this background radiation daily, since the formation of Earth. In a year, each of us gets about 200 mrem radiation from this background radiation.



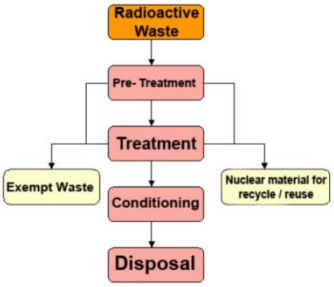
The fourth case is the exposure to radiation for medical and other reasons. Mankind needs nuclear radiation for many uses like diagnosis of diseases, treatment of cancer, screening of seeds, increasing the shelf life of food items including vegetables, and so on. For example, onion can be stored fresh in normal sealed bags for more than 7 years if they are irradiated.

The wastes from nuclear power plants have been points of concern for the common man since the experts and scientists in the field have not come out in the media and on the street to explain with authority to the common man about the precautions and safeguards, in as sure terms as we do about science and technology.

Characteristics of Radioactivity

One characteristic of all radioactive wastes which distinguishes them from the larger quantity of other toxic industrial wastes is that their radioactivity progressively decays and diminishes. For instance, after 40 years, the used fuel removed from a nuclear reactor has only one thousandth of its initial radioactivity remaining. All radioactive waste facilities are designed with numerous layers of protection to make sure that people remain protected for as long as it takes the radioactivity of these nuclear wastes to reduce to 'background radiation levels of Earth'.

Three Kinds of Waste



Radioactive waste can be in gaseous, liquid or solid form, and its level of radioactivity varies. The waste can remain radioactive for a few hours or several months or even hundreds of thousands of years. Depending on the level and nature of radioactivity, radioactive wastes can be classified as Exempt Waste, Low andIntermediate Level Waste, and High-Level Waste. When the spent fuel is subjected to chemical processing, itresults in three kinds of waste — Low-Level Radioactive Waste (in high volumes), Intermediate-Level Radioactive Waste (intermediate volumes), and High-Level Radioactive Waste (low volumes).

If the High-Level Waste is reprocessed, 97 per cent of this can be recycled into depleted Uranium and about 230 kg of Plutonium, which can be made into mixed oxide fuel (MOX) and used. This leaves about 700 kg of High-Level Waste a year, which needs to be environmentally isolated for a very long period of time.

Isolation is achieved by converting the High-Level Waste into glass-like solid cakes (vitrification) of about 4.8 tonnes, stored in steel canisters. Extreme care is needed in processingthis highly radioactive material, and specialised facilities are necessary.

Low-Level and Intermediate Level Waste will lose their radioactivity in 50 years; High-Level Waste may take more than 10,000 years. After storage for about 50 years, these canisters can be put into deep underground (more than 3000 feet below the seal level) repositories for long-term storage.

High-Level Waste of 700 Kg after vitrification may weigh around 4.8 tonnes. A minimum of 450 tonne High-Level Waste is necessary for deep underground storage. This vitrified waste is therefore kept in Spent Fuel Storage Facility safely within the same premises. Since India has only a low level of production of nuclear energy, keeping the vitrified waste underground may take a longer time. Till such time, the vitrified waste will be accumulated and stored within the same premises safely.

America's Plan to Store High Level Nuclear Wastes

Plans to store the majority of America's spent nuclear fuel and other highly radioactivewaste at a central repository underneath Yucca Mountain in the Nevada desert 80 miles from Las Vegas are under active consideration. The effect of various natural forces such as erosion and earthquakes are being analysed. The design of the site, as of now will be safe for 10,000 years and the design is now being upgraded for a safety duration of 1 million years. The Federal Nuclear Regulatory Commission (NRC) aims at the proposed facility to "stand up to any challenge anywhere," adding that issues of health safety have been a primary concern during the planning process.

The Indian Scenario

Many debates are going on in India about the safe disposal of nuclear waste. Many activists and political leaders are on the streets, protesting against the storage of nuclear waste. Unfortunately, the protestors do not seem to have understood the concept of 'spent fuel storage' and 'nuclear waste storage'. Even

the Atomic Energy Department and the Nuclear Power Corporation have done little to create awareness about this to eliminate the fear among the people.

Presently, India has 22 nuclear reactors in 7 sites, generating 6780 MW power. Construction is in progress to generate 4730 MW more power. The Government aims at 63000 MW generation of nuclear power by 2032.

Currently, Uranium is used as fuel in all the nuclear reactors. India is the only country which has developed the technology to generate power using 'Thorium'. India has more than 6 lakh tonnes of Thorium, the second richest resource in the world. In another 15 to 20 years, India will start using Thorium as fuel.

Since India generates only around 6.7 GW of power, the country is not yet facing the challenges of nuclear waste storage. However, due to lack of awareness, some of the activists and the media are creating unfounded fear in the minds of the people.

Spent Fuel Management

In March 2004, The Atomic Energy Regulatory Board (AERB) issued comprehensive guidelines on waste management for nuclear power plants using ***Pressurized Heavy-Water Reactors (***PHWR), which were the mainstay of India's programme. These guidelines cover all aspects of waste management including transport, storage and disposal facilities. Each plant is to set up its waste management organisation, plant, and related facilities before commissioning.

The scheme for the storage of spent fuel in a nuclear plant is two-fold – one facility is located within the reactor building/service building, generally known as the Spent Fuel Storage pool/bay, and the other is located away from the reactor called the Away From Reactor (AFR) Spent Fuel Storage Facility, but within the plant's premises.

A 1000 MW reactor produces 25 tonnes of spent fuel a year. As per the guidelines of the Atomic Energy Regulatory Board (AERB), the

25 tonne Uranium road is stored in 'Spent Fuel Storage Facility' within the same premises of the reactor under water for about 5 years. During this period, the radioactivity decreases. Former Indian President Dr APJ Abdul Kalam used to describe the nuclear waste as an "Asset", as this can be recycled and reused.

Conclusion

Now mankind is at the threshold of mastering nuclear fusion technology. If we achieve this, then we can all get clean energy from nuclear fusion reactors. At that time, probably a jar of water can generate enough electricity for the entire city of Mumbai for one full year and that too without any radiation risk! Until that and other promising alternative energy sources emerge, we will be concerned about the long-term safety of storing the nuclear wastes from all our fission reactors around the world.

by K Srinivasan, Publisher & Managing Editor,
& Prof R Jagannathan, Editorial Advisor
(With input from Shri V Ponraj, Former Advisor to Dr APJ Abdul Kalam)
Source : Junel 2019 issue of PreSense

*****

Welcome 5G!

It is quite fashionable to use the term, or to be precise, the suffix "G" these days, to denote "Generation". It has become common too, to call anything which is latest, as "Next Gen", whether it is technology-based or something totally different. It is therefore no wonder that the suffix G gets attached to network architecture and technology like 2G, 3G, 4G and now the widely spoken about 5G.

Transition of 1G to 5G

In network technology, the earliest communication technology, later called 1G, referred to a network speed of 2.4 Kbps which is the speed of transmission of 2.4 kilobits per second *i.e.* 2400 bits of data per second, ('k' referring to approximately 1000 or precisely 1024).Later on, 2G offered 64 Kbps. 3G was used to denote 144 Kbps and the recently introduced 4G is 100 Mbps (Mega ie 1000 kilobits per second) speed upto 1 Gbps (gigabps)*i.e*. 1000 Mega.

The computer moves data in bits denoted by small "b". Capital "B" refers to 'byte' which is a character represented by a combination of eight bits of either zeros or ones and is used in storage and memory. In other words, computers store data in bytes and moves it in bits.

Technology pundits have not yet come to a finite conclusion on how to define 5G. Like any field with rapid advancements, network technology too is progressing not just fast but extremely fast. People say that 5G is no doubt the latest in network transmission technology and a giant leap (until of course, the next generation comes up with enhanced features to be called again the *latest!*). 5G is expected to provide upto 20 Gbps speed with millimetre

waves of 15 gigahertz (in internationally accepted system of units it is 15 billion cycles per second) and even higher frequency.

What is 5G?

Although the term 5G is often referred to in broader terms with technologies than just network speed, we often associate it with network bandwidth. However, it is not just speed. It includes other issues like software, waves and latency that are also to be studied and understood in the context of 5G. Latency, a term often discussed with network speed, denotes the delay before a transfer of data begins, following an instruction for its transfer from the computer system. To reap the advantage of 5G in mobile communication, it does not suffice if the mobile network operators alone provide it. The devices too should be compatible with the 5G technology.

Deployment

From a technology perspective, it is not just the mobile devices but the Internet of Things (IoT) much wider than mobile communication, which has much to cheer as an industry. People even say that much more than the network and other industries associated with it, it is the IoT hardware industry which pushes for the 5G technology. With the increasing popularity and deployment of IoT devices (not just computers and mobile) being accessible with an IP address like printers, microwave oven, toys, cars and all such devices, it is this IoT market that will benefit mostly by 5G. In the next couple of years, if the global players arrive at a consensus for technological standardisation, which is most likely to happen, smart cities management, agriculture planning, weather forecasting, academia and virtual reality (which is even expected to replace the existing GPS)will all be 5G-enabled. 5G in non-mobile communication (like IoT devices) may function at a reduced speed and not at the speed for cellular devices. Speed will certainly be a matter of concern in critical IoT devices like remote surgery at corporate hospitals and real time traffic management on which research and trials have already started.

In India, Ericsson has already reportedly set up a hub in New Delhi for its 5G innovation and most of the major telecom players are also planning their deployment strategies. 5G spectrum and its sales or auction among the network players in the country will soon take place, as per the government's policy in a manner such that the technological issues are addressed, security concerns are taken care of, legal redressal is provided and political ramifications are adequately studied. TRAI has to regulate, manage and monitor the transition from 4G to 5G as a matter of policy. Device makers and cellular operators are getting ready, since it is expected that 5G will operate on higher frequencies, even upto 28GHz.

(Image Source: www.electricalfundablog.com)

The Indian industry is quite optimistic about the massive deployment of 5G since the existing WiFi has a distance constraint of around 50 metres compared to which 5G would be easy to handle, with smaller antennas or such easily manoeuvrable devices, reaching out to not just the mobile phones but many other equipment like cars, motor cycles, surgical equipment, printers and all sorts of machinery and hardware items.

Since the mobile-cellular industry has been a funds generator, accelerating economic growth, its influence (much more than that of IoT) is expected to be huge in our country. TRAI has to decide on the spectrum allocation for 5G enabling its massive deployment, at an affordable rate and yet regulating the mobile industry with Information Technology Ministry simultaneously putting in place the regulatory, legal and mandatory guidelines to bring all IoT devices, the entire technology including the hardware, software and the network component and not just the mobile industry, under its umbrella.

Perhaps it is this massive deployment of 5G that causes concern among a section of activists about invasion into privacy of data through the devices, doctors getting worried about the human health aspects of 5G rays, scientists getting anxious about its

impact on environment and of course the common man worried about the psychological impact including an aggravated addiction on human minds. But then, that is technology – once it arrives, there is no stopping it. Let us wait and watch.

by V Rajendran, Editor
Source : July 2019 issue of PreSense

*****

Beware and Be Aware of Mobile Phone Vulnerability

The smartphone has penetrated our daily life so much that one cannot now think of life without it. People use smart phones for the social media and other applications too. It is a matter of constant debate as to what extent the data stored in smartphones are safe and protected from hacking. The reason for this concern is that every user is in the habit of downloading many mobile apps from different sources after ticking the mandatory 'yes' in order to do so, thereby providing permission to the app providers in most of the cases, to access all the files or data in the mobile.

To understand the extent of the vulnerability of the smartphone to these mobile apps, PreSense Team consulted experts who highlighted the gravity of the matter.

Hacking

The hacker (generally called a security hacker, who is one who uses his technical skills to gain unauthorised access to systems or networks to commit a crime) can gain access to someone else's mobile phone after identifying the vulnerabilities in the mobile phone. Experts opine that even branded mobile apps are safe only to the extent of about 80%.

Rogue hackers can misuse the hacked phones to access the victim's personal information and sell it to business vendors. They can also gain access to private and confidential information like photos for unethical exploitation.

The Amazon billionaire, Jeff Bezos had his mobile phone 'hacked' in 2018 after receiving a WhatsApp message that had apparently

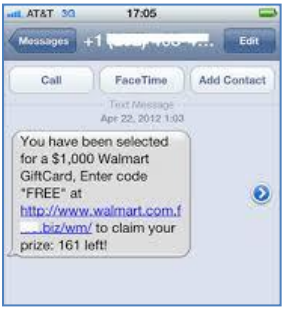
been sent from the personal account of the Crown Prince of Saudi Arabia, according to the report published in the Guardian. The encrypted message from the number used by Mohammed bin Salman is believed to have included a malicious file that infiltrated the phone of the world's richest man, according to the results of a digital forensic analysis. Therefore, companies keep testing their applications and patching the loopholes to provide maximum safety.

How are Malware Apps Planted?

Experts say that it is safe to download apps from Google Play Store or App Stores (in the case of Apple phones). Unfortunately, mobile phone users tend to download various mobile applications from untrusted and unverified sources too.

In case of apps installed from third party play stores, hackers are able to bind their malware app to the legitimate app and compromise the authenticity of the apps. Hackers can then remotely install their apps in target mobile phones through the IP address. They take control of the targeted mobile device to perform any action like remotely making a call from it to others, accessing the camera, stealing data from the mobile phone, etc. Since the victim will also be able to operate the mobile device, he might not be aware that his mobile is hacked and under the control of someone else.

How do Hackers Attack?



There are several methods by which hackers attack the target device. Some of the popular methods are:

1. Sending a link through SMS. When the victim clicks the link for access, the hacker gains control of the mobile phone. *(See image).*
2. The hacker can install an app in the target device by gaining physical access of

the phone. It is therefore not safe to hand over the phone to a stranger.
3. The hacker can access the target mobile through SIM card cloning, after gaining physical access to it.
4. The hacker can make a call to the target device. When the victim attends the call, the hacker is able to gain control of the mobile phone by clandestine installation of a malware at that time.

Banking Applications in Mobile

People use online payment apps for money transactions. It would normally be difficult for the hacker to access the victim's account unless the victim himself shares the password/PIN. If the mobile is hacked and brought under the control of hacker, then it is also possible for the hacker to transact through the banking apps after gaining access to the password if it is stored somewhere in the phone. Hackers are usually caught in action while making a transaction after hacking.

Banks hire security professionals to find out possible vulnerabilities in their apps. Security experts admit that even in their endeavour to give maximum possible security to the world, 100% safety and security in the cyber world is impossible.

Ways to Find Out Whether the Mobile Phone is Hacked

1. The users will observe unexpectedly poor performance in their device. The home page will have the icon of rogue apps.

2. The user can install an app 'No root firewall' from Google Play Store and monitor the installed applications. Internet security applications can also be installed.

3. If the battery drains out fast, it may be an indication that it is bugged and someone is uploading the data from the mobile phone without the user's knowledge.

If the user finds that his mobile phone is hacked, he must take it immediately to a cyber security expert or the mobile manufacturer.

Caution Against Selling Used Mobiles

If the user intends to sell his used mobile phone, he should first re-format his mobile phone before the sale. If the mobile phone contains any personal or private photos, then it is preferable not to sell it because each and every data is recoverable using 'recovery tools', including system logs, even after re-formatting. If the user has any bank account that is accessible through the mobile phone, then too, it is better to re-format the mobile phone before selling the phone. The passwords of the bank accounts and email accounts should also be changed immediately.

How to Avoid Being Hacked

1. Download mobile applications from Google Play Store or manufacturer's authorised App Stores only. Avoid downloading applications from third-party sources. In 'settings', disable 'third party source'.
2. Avoid pre-installed applications from third party sources.
3. Do not click on links from unidentified sources. Avoid accessing short URLs as they may take the user to malicious sites.
4. Use stickers to cover the camera in the mobile when not in use.
5. Do not allow anyone to scan the QR code from the mobile phone. It will result in compromising the WhatsApp privacy.
6. Quick Response Code Login Jacking (also known as QRL Jacking) is a social engineering attack by which the attacker can hijack the session, affecting all applications that depend on the "Login with QR code" feature as a secure way to login to their respective accounts.

Types of Malicious Emails

7. Key-in the website URL directly into the browser to log in. Logging in through text links received from unknown sources should be strictly avoided.
8. Be aware of malicious emails received in the inbox (*see image on right, as illustration*). Avoid clicking any link given there.
9. Avoid giving the mobile device to any stranger.

One can type one's email ID in the following link: https://haveibeenpwned.com/ to check whether the email ID is included in any hacked websites' database.

Health Hazards of Excessive Mobile Phone Usage

Incidentally, excessive use of the mobile phone has its health hazards.

The Federal Communications Commission (FCC) has adopted the limit of 1.6 watts per kilogram (1.6 W/kg) as safe exposure to radio frequency (RF) energy. This is known as SAR (Specific Absorption Rate). Any smart phone with a reading upto this SAR level is deemed 'safe' for use. Even then, use of the phone for an extended time period is still hazardous to the health.

Check if your email or phone is in a data breach
https://haveibeenpwned.com/

The user can check the radiation level of the smart phone in terms of SAR by dialling a USSD code *#07#. If the result shows SAR below 1.6 watts per kilogram (1.6 W/kg), then it is safe for use. If the SAR value is higher, it is advisable to change the device immediately. Using such a phone with high SAR even for a limited time period is hazardous to health because of the high intensity of radiation.

Conclusion

With technology growing at such a fast pace, cyber-crimes are bound to grow at an even higher rate. With technology here to

stay, it is then the responsibility of every mobile phone user to ensure that his/her device is kept safe from the attack of hackers.

by K Srinivasan, Publisher and Managing Editor
with input from V Pradhan, Ethical Hacker, Chennai.
Source: February 2020 issue of PreSense

*****

Government Should Improve the Ecosystem to Encourage Innovation

The latest Innovation Index for 2019 indicates that India is in the 52nd position among 129 countries on the basis of 80 indicators measuring various aspects of innovation. Even Singapore (ranked 4) and China (ranked 14) are above us. Although it can be argued that we have improved our ranking from 81 in 2015 to 52 in 2019, we need to understand that unless the Government comes out with a concrete policy to encourage innovation, it would be difficult for India to improve the position further.

There is a general feeling among the people that Indians do not have enough competencies to compete at the global level and innovate products. It is not so. For thousands of years, Indians have been recognised as highly knowledgeable, and have been experts in various domains like mathematics, chemistry, medicine, astronomy, engineering, architecture etc. Where did the knowledge go? Why are Indians not able to bag Nobel Prizes?

Many people are not aware that more than 928 multinational companies (MNCs) have hired nearly four lakh processionals within India to do Research and Development (R&D) Projects. Many leading MNCs like IBM, Microsoft, Google, Oracle, Adobe, etc. hire talents within India and also outsource to Indian companies like Wipro, HCL, Dr Reddy's Lab, etc. These MNCs spend more than 40% of their global spending on R&D within India. This clearly indicates that Indian professionals are highly competent to match the global standards. It is also said that IBM has more than 60% of its employees as Indians. Indians are heading Microsoft and Google. Our Indian professionals develop products for the foreign companies and they market them under their brand name. India is buying these products at high costs.

In spite of Indian professionals creating world class products, India does not have software or hardware products which are marketed globally under an Indian brand. When we interacted with several renowned academicians across the country, they all admitted that notwithstanding the assurance by Prime Minister to increase the scope for innovation, the ecosystem is not conducive to the potential innovators.

It is estimated that around 1 lakh crore of rupees is spent annually on Research and Development in India. Of this, 55% is consumed by the Central and State Governments. 38% is used by the private sector. 4% is used by the higher education institutions. The Government spends the amount on defence, space, and electricity related research projects. The private sector uses it mainly for pharma and transportation projects. Many academicians feel that the 4% spent by higher educational institutions is poor, when compared to developed nations.

A former Vice Chancellor of a University and scientist said that there was no point in increasing the funds, unless the quality of the teachers and education in higher education institutions is improved. He added that prior to the 1980s, persons passionate about education used to join the teaching job. Nowadays, many of those who cannot get better jobs get into teaching. Indian researchers in educational institutions bring out a large number of articles for journals, but most of them are of poor quality. He

added that in order to improve the quality of students, an all-India entrance examination must be initiated for engineering too, like NEET (National Eligibility cum Entrance Test) for medical stream, so that future projects of India, in all disciplines are handled by quality people. He hoped that the new education policy planned by the Government would address this issue.

Another senior professor of Indian Institute of Technology said that he had submitted 8 documents for patenting some of his innovations. The authorities took up the examination of one product after four years. The remaining 7 products are pending with the authorities for the past five years. Even the competence of the examiners is highly questionable. Many innovators prefer to file in India for patents as it is cheaper to do so. But the inordinate delay and the incompetent examiners discourage them from filing their documents in India. The professor added that he has advised some of his students who work in USA to file their patent documents there itself even though it is costlier. They get the approval within six months. Unless the Government improves the ecosystem, many of our innovators may not be comfortable about filing their patents in India. Filing them in USA is not practical for most of the innovators.

In 2015, Prime Minister gave a call to all PSUs (Public Sector Undertakings) to collaborate with high-end institutions for innovation. It is not known to what extent this has become successful. The incubation centres in IITs and NITs are successful. This can be doubled to accommodate more innovations.

In India, we are not in the habit of celebrating the great scientists, as we do with film stars and politicians. An Indian scientist, who was not found eligible for a tutor's job by an Indian University, went abroad and became a Nobel Laureate. Today, we laud him as an Indian. Do we have any moral right to take credit for his success? All Indian-born Nobel Laureates were supported by foreign countries to achieve their goal. We have the history of driving them out of our country, citing various rules. It is suggested that we can name or rename some of our Universities after some of the Indian Nobel Laureates and other great Indian scientists, so that present Indian youth are inspired.

PreSense appeals to the Government of India and the Standing Committee on Science and Technology to examine the urgent need for improving our ecosystem in order to motivate young Indian innovators to develop products for India.

by K Srinivasan, Publisher and Managing Editor
Source: June 2020 issue of PreSense

*****

Ozone Layer – Saviour of Life on Earth

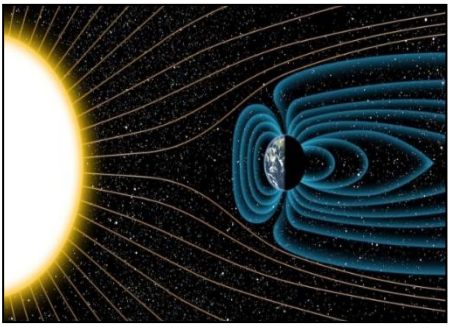
Introduction

Life on earth evolved from some basic chemicals, conducive environment and some definite processes. Earth was formed about 4.5 billion years ago and evidence suggests that life emerged more than 3.7 billion years ago. Approximately one trillion species currently live on Earth!

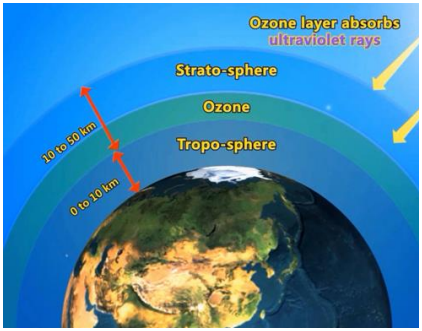
The depletion of the ozone layer, which is present at a height of about 15 to 35 kilometres in the atmosphere, poses a great threat to all life forms on Earth. In a concerted effort to bring about an awareness, 16th September is commemorated as the International Day for the Preservation of Ozone Layer.

Constant Threat to All Life Forms on Earth

Although our Earth is at an approximate distance of 150 million kilometres from the sun, the constant radiations emitted by the sun and the entire cosmos on a 24X7X365 basis is sufficient to kill all life forms on Earth within a few days' time. The Earth and its life forms are protected from the danger of radiation by two components. The Earth's magnetic field protects us from the intense stream of charged particles (alpha and beta). The Ozone layer protects us from the dangerous UV-c and most of the UV-b radiations from our sun (*see images below*).



Earth's Magnetic Field



Ozone Layer over Earth

The Ozone Layer and How it Works

Ozone is present in the normal air that all of us breath at our homes and in open air. But its abundance is so low that we do not smell it. It is only about 0.3 parts per million in all our cities. Ozone by itself is a pale blue poisonous gas. But at a height of 15 to 35 kilometres, the concentration of ozone is about 35 times greater. Ozone at this concentration, permits the visible light and overlapping harmless UV-a radiation from sun to reach the Earth. Ozone absorbs 99.7% of the UV-b radiations and permits only about 1/350 times the incident of UV-b radiation to reach Earth so that we are safe, and at the same time are able to synthesise enough Vitamin D without getting sunburned. The Ozone layer completely thus absorbs the harmful UV radiations from the sun and protects all life forms on Earth.

The Ozone molecule absorbs the UV-c radiation and most of the UV-b radiation from the Sun to become an oxygen molecule and a single oxygen atom. They combine again to form the ozone molecule. Thus, the recycling recurs continuously and, in the process, the ozone layer is sustained around the Earth. This process produces some heat, which is passed on to Earth, which re-radiates this heat back to outer space. The net result is that all life forms on Earth are protected from the dangerous effects of solar radiation.

Ozone Hole – Creation and Consequence

The Ozone hole is not really a hole. It is only a reduction in the concentration of Ozone. It is a depletion where chlorine is the main culprit.

Chlorine has many uses. It is used in swimming pools and drinking water to kill bacterial and fungal contaminations. Gaseous chlorine dioxide is used to decontaminate enclosed spaces and equipment. These chlorines are not a threat to ozone layer since they are water-soluble and do not rise to the stratospheric heights.

But researchers have found that the chlorinated species, primarily from manufactured compounds like the Chloro Fluro Carbons (CFCs), carbon tetrachloride, methyl chloroform, and the hydrochlorofluorocarbon (HCFC) substitutes for CFCs rise to the stratosphere.

Researchers have found that the emissions of the human-produced halocarbons, plus the much smaller contribution from natural sources, could account for all of the stratospheric chlorine. They found that the increase in the total stratospheric chlorine measured, corresponds to the known increases in the concentrations of human-produced halocarbons.

The presence of these man-made chemicals and chlorine in the stratosphere are harmful in two ways. Firstly, they convert the ozone molecules into normal oxygen molecules irreversibly so that the ozone protection to earth is gradually depleted, exposing us all to harmful radiations. Secondly, the presence of these man-made chemicals in the stratosphere forms a greenhouse shield around Earth, which reflects the heat radiated by Earth, back to Earth.

This prevents Earth from cooling itself as a natural process. This causes the harmful global warming, polar ice-caps to melt, sea-levels to rise, and endangerment of aquatic life.

India and the Ozone Layer

As per the National Ozone Centre in New Delhi, there is no trend to show total ozone depletion over India. A network of stations that measure total ozone some six times a day, covers Srinagar, New Delhi, Varanasi, Ahmedabad, Pune and Kodaikanal.

The incidence of skin cancer across India is also monitored. There are controlled studies to observe the effects of changing UV-b radiation concentrations on crops.

Conclusion

The Ozone layer enveloping our Earth is a life-protecting shield provided by nature. Unfortunately, man-made chlorine-based chemicals are destroying that shield. The reversal of this trend and discovering alternate chemicals for the various uses are the challenges to mankind in the effort to survive well for generations to come. It is hoped that mankind will win the challenge.

by Dr R Jagannathan, Editorial Advisor
Resource Input: International Agency Reports and Research Agencies.
Source: June 2020 issue of PreSense

*****

The Nobel Prize and Nobel Laureates 2020

The most coveted prize on Earth, the Nobel Prize is awarded every year, on 10th December, to the "Laureates" who have contributed "the Greatest Benefit to Mankind" in Physics, Chemistry, Physiology or Medicine, Peace and Literature.

A Flashback

Birth of Nobel Prize: On 27th November 1895, a year before his death, Alfred Nobel signed the famous will which would implement some of the goals to which he had devoted so much of his life. Nobel stipulated in his will that most of his estate, more than SEK (Swedish Krona) 31 million (which is approximately SEK 1,702 million at today's value, and roughly equivalent to 1481 crores of Indian rupees) should be converted into a fund and invested in 'safe securities'. The income from the investments was to be "distributed annually in the form of prizes to those who, during the preceding year, have conferred the greatest benefit to mankind." Since 1901, the Nobel Prize is conferred under five categories by Swedish and Norwegian committees in recognition of advances made in the fields of Physics, Chemistry, Physiology or Medicine, Literature and Peace.

The related 'Nobel Memorial Prize in Economic Sciences' was established by Sweden's central bank in 1968.

The Most Respected Selection Process: Nomination forms are sent by the Nobel Committee to about 3,000 individuals, usually in the month of September of the year before the prizes are awarded. These individuals are generally prominent academics working in the relevant field of specialisation. The deadline for the return of the nomination forms is 31st January of the year of the award.

The Nobel Committee nominates about 300 potential laureates from these forms and additional names. The nominees are not publicly named, nor are they told that they are being considered for the prize. All nomination records for a prize are sealed for 50 years from the awarding of the prize.

The Nobel Committee then prepares a report reflecting the advice of experts in the relevant fields. This, along with the list of preliminary candidates, is submitted to the prize-awarding institutions. The institutions meet to choose the laureate or laureates in each field by a majority vote. Their decision, which cannot be appealed, is announced immediately after the vote. A maximum of three laureates and two different works may be selected per award. Except for the Peace Prize, which can be awarded to institutions, the awards can only be given to individuals. The Nobel prizes are not awarded posthumously.

Nobel Prizes and Laureates 2020		
Nobel Laureates	**Field**	**Contribution**
Harvey J. Alter, Michael Houghton and Charles M. Rice	**Medicine**	Discovered Hepatitis C virus
Roger Penrose	**Physics**	Discovered that black hole formation is a

		robust prediction of the general theory of relativity
Reinhard Genzel and Andrea Ghez		Discovered supermassive compact object at the centre of our galaxy
Emmanuelle Charpentier and Jennifer A. Doudna	**Chemistry**	Discovered the method for genome editing
Louise Glück	**Literature**	For her unmistakable poetic voice that with austere beauty makes individual existence universal
World Food Programme (WFP)	**Peace**	For its efforts to combat hunger, for its contribution to bettering conditions for peace in conflict-affected areas and for acting as a driving force in efforts to prevent the use of hunger as a weapon of war and conflict.
Paul R. Milgrom, Robert B. Wilson	**Economic Sciences**	For improvements to auction theory and inventions of new auction formats.

In 2020, there is a record number of four women Nobel laureates. PreSense congratulates all the Nobel Laureates 2020.

by Professor Dr R Jagannathan, Editorial Advisor
Source: November 2020 issue of PreSense

*****

Security of Women in the Digital Space

Digital Security Association of India (DiSAI), an initiative of your eMagazine PreSense organised a Webinar on 'Security of Women in the Digital Space' on 11th January 2021.

Dr M. Ravi, IPS, Additional Director General of Police (ADGP), Special Task Force, Erode, Tamil Nadu State, addressed the participants, which included practising advocates, law students and cyber security professionals He took the audience through the *modus operandi* in various cybercrimes, especially those concerning women. He kickstarted his session by explaining about the digital space, the indispensability of a mobile phone, the vulnerabilities while using a smartphone, and the usual risk areas and situations where women fall victims, in the digital space.

Dr Ravi described some of the cases he had handled in his long career with the Tamil Nadu Police, particularly those relating to the investigation and prosecution of crimes against women. Drawing from his rich experience in cybercrime investigation and techno-legal issues concerning women and children, he stressed the importance of alertness and awareness about the different facets of crimes in digital space. He spoke about email spoofing, cyber stalking, and child trafficking, and elaborated about the efforts taken by the police in the country with particular reference to Tamil Nadu, in tackling the crimes against women in social networking sites.

Excerpts From his Talk:

Security of Women: Day by day, more women than men, are browsing the Internet and are active in social networking sites. It is reported that around 27% of the women in the cyber space, have been stalked at some point. Therefore, awareness about the possible risks and threats is the essence. Women should know what could be disclosed in a social networking site, how to keep

their private information safe and secure, and how to exercise caution by taking some basic, simple steps, like never disclosing any personal information in social networking sites, not chatting with strangers, not keeping the GPS enabled, exercising restraint about sharing any information in any app, not browsing the internet randomly without a proper device security app installed.

All-Woman Police Stations: There are all-woman police stations in many places in the state. Each of these stations is well-equipped with trained personnel to take care of women safety, maintain the anonymity of the women victims/complainants, handle cybercrimes efficiently, and deal with all kinds of women-related crimes occurring in the society. All such stations are provided with facilities like child-friendly corners to make children victims feel comfortable, and a speedy grievance mechanism on a 24X7 basis. They initiate pro-active steps of tracking down previous criminals with recorded history while tracing culprits. In spite of these women-friendly facilities, many women hesitate to approach the police for fear of adverse publicity. There is however, a marked improvement in this attitude, with more women approaching the police for help and redressal.

Assistance Provided by Tamil Nadu Police: There are several helpline numbers for women in distress to contact in times of need or crisis, or as SOS. In addition to the general police helpline number of 100, there are other helpline numbers like 181, 1091, etc., and specific numbers of top police officials in the major cities of Tamil Nadu.

The Kavalan SOS app, developed by the Tamil Nadu Police, is a user-friendly app that can be used, to contact the police in times of distress. It is becoming a popular app in use among women. It works 24X7, with a team of alert, agile and well-informed police

officials available on call. The moment an SOS or a distress call is sent through the Kavalan app, it instantly reaches the police. In prompt response, the police take immediate action to track the caller with the help of GPS, and alert the nearest police station or patrol police, so that a rescue team of police arrives at the distress spot within a few minutes. The police have been receiving positive, encouraging and appreciating public feedback about the efficiency and effectiveness of the Kavalan app.

Practical Difficulties While Investigating a Cybercrime: Dr Ravi said that when cybercrime is committed by a person who is abroad, even though detection is easy, the actual task of bringing the culprit to our court of law is a cumbersome process. We have to approach the Ministry of Home Affairs, and then take the assistance of INTERPOL to try to extradite the criminal. If the criminal is not an Indian but a foreign national, the issue could become more complex.

Crime Against Children: Many initiatives have been taken by the police to create awareness among children, both boys and girls, about crimes committed against children. The police also educate boys about how they could be innocently used, to be part of a criminal gang. The police pay equal attention to educating adolescent boys, who are as vulnerable as girl children.

Use of Smartphone: With the wide penetration of smartphones and the indiscriminate use of all kinds of apps in the smartphones, especially by people with insufficient basic knowledge about its use, the security of data is compromised. Privacy is also compromised to a great extent in the digital space. Therefore, users should be sure about the necessity, authenticity and safety of the apps before downloading them. Smartphone users should be adequately aware of the prevailing and common cybercrimes like phishing, email spoofing, cyber stalking, key-logger software, password theft, and such acts, to safeguard against them. People should not blindly believe anything that comes in a social

networking site. Of late, fake news about employment opportunities and matrimonial offers are abundant, and people are being duped to part with their money without verifying the credentials of the person making such offers in the internet.

Awareness, and vigilance is the key to the safety and security of women and children, and men, be it in real life or in the virtual world of cyber browsing.

The complete interview can be watched in the link: https://youtu.be/WNV6IYcEuv0.

by V. Rajendran, Editor
Source: November 2020 issue of PreSense

*****

Satellite Navigation

Man is a social animal, and navigation as well as communication is an inherent urge in any human being. Being primitively nomadic, human beings, like most other species in the animal kingdom, were compelled to move from place to place in search of food and sometimes away from threats and enemies. With time and experience, human beings learnt to rely on familiar landmarks, and the direction of the celestial bodies, to earmark their position, in the course of their journey.

History

Indian history is full of stories on how emperors navigated and moved from one territory to another, in their quest to conquer kingdoms. Around 1000 years ago, King Rajendra Chola of the Chola Dynasty in Tamil Nadu (now the delta region of the state) travelled to South East Asian kingdoms and regions (now called Sumatra, Burma and Cambodia). Chinese travellers have travelled to India, and many Indians have travelled across the seas on specific missions like trade, conquest, expeditions, religion and so

on. The Indian sage, Adi Sankara travelled from South Kerala to the northernmost part of India, *viz.* the highlands in Kashmir and set up a temple there.

When men began to use the seas to explore new lands, they used to sail alongside the shoreline and look for landmarks that told them of the progress in their journey. When they began to sail far out into the seas and out of sight of the land, they relied on the direction of the sun during the day, and the North Star and other constellations during the night. Interestingly, some even followed the direction of birds' flights, or of the fish that swam. Then came the invention of the compass which is based on the magnetic fields of the earth, to show the directions.

By the 19th century, electronic navigation tools such as calculators and computers made reading directions easier, and travel more convenient. Navigation has come a long way over the centuries. Today, we have satellite-controlled and -monitored aids to facilitate navigation as well as communication across the lands and seas, and even across the universe within the solar system. Almost all navigations and communications are enabled by navigation satellite systems that relay from Earth's orbit to terrestrial stations, for use by the people.

Global Navigation Satellite System (GNSS)

GNSS refers to a constellation of navigation satellite systems providing signals from space, to transmit positioning and timing data to GNSS receivers. The receivers then use this data to determine the location. GNSS is the generic term for satellite navigation systems for global coverage. RNSS stands for Regional Navigation Satellite System for regional navigational coverage. The advantage of having access to multiple satellites is accuracy and accessibility at all times. Even though satellite systems do not generally fail, in case of such an eventuality, or if the line of sight from any one satellite is obstructed, the GNSS receivers can pick up the signals from the other satellites on standby.

The primary operation of the GNSS is to transmit carrier waves which bear information, from the satellites to the receivers on

Earth. A GNSS receiver has two elements comprising an antenna and a processor. The antenna catches the signals while the processor decodes and makes sense of the information received. To know the accurate location, the receiver needs to process the signals transmitted from a minimum of three satellites.

GPS or Global Positioning System

To the common man, the word GPS or Google Maps is a familiar term, used to locate directions or routes. GPS is one of the four Global Navigation Satellite Systems (GNSS), available today. The motorist, who is looking for the direction and the route to reach his destination using the Google Map, is familiar with GPS. It is also used by a person to indicate where he is, by giving his address, that is deciphered and recognised by GPS to pinpoint his location.

GPS was developed by the US government, initially for their military navigation. It is maintained by the US Air Force, and is the oldest GNSS. The US government initiated its operations in 1978 and it was later on, that it was made available for civilian use. GPS can be used by anyone with a GPS device, which receives the signals from the satellites.

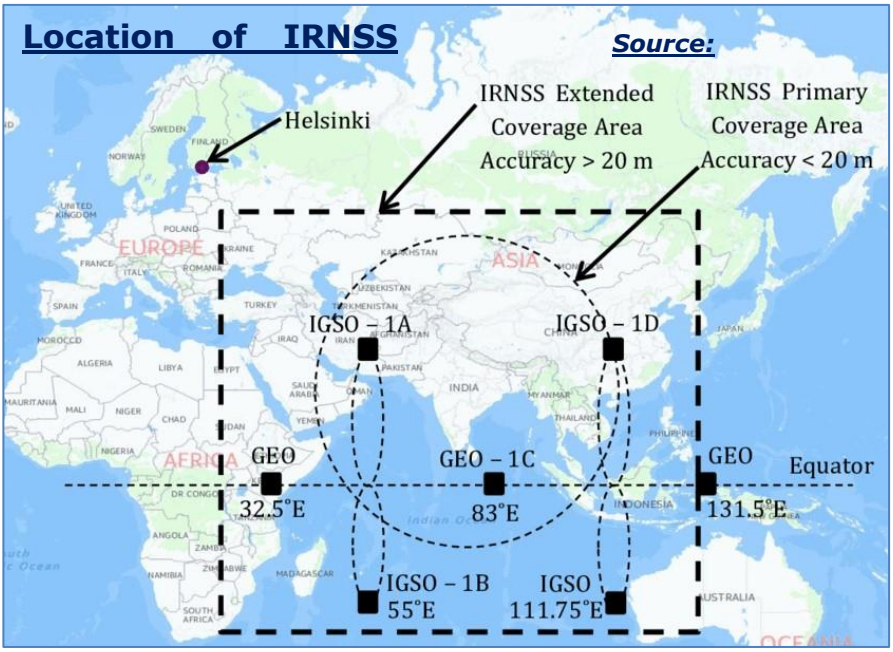
How does GPS work?

GPS is a network of about **31 satellites** orbiting Earth at an altitude of around **20,000 kilometres.** Each satellite of the GPS constellation circles Earth twice a day. **Twenty-four satellites** currently function to provide the accurate location, while the remaining five satellites are spare ones.

Wherever you are on Planet Earth, at least four GPS satellites are 'visible' at any time. It requires only three satellites to provide the location. The other satellites add to the accuracy of the reading of the location. Each satellite transmits information about its position and the current time, at regular intervals. Travelling at the speed of light, these signals are intercepted by a GPS receiver, to calculate the distance from each satellite.

Soon, more countries developed and sent their own GNSS constellations into the orbit round Earth, for navigation and location purposes. Currently, there are four global GNSS systems *viz*. GPS (US), GLONASS (Russia), Galileo (EU), and BeiDou (China), and two regional systems *viz.* QZSS (Japan) and IRNSS or NavIC (India).

Indian Regional Navigation Satellite System (*IRNSS*)



IRNSS or NavIC (acronym for Navigation with Indian Constellation), is an indigenously developed regional satellite navigation system that provides accurate real-time positioning and timing services. Incidentally, the Sanskrit word *nāvik* means 'sailor' or 'navigator'. IRNSS was designed by the Indian Space Research Organisation (ISRO). While GPS has 24 functional satellites to service the entire globe, IRNSS has 7 satellites, modelled to provide regional location information service, covering India and its neighbouring nations in an area extending upto a

radius of 1,500 kilometres from the Indian boundary, at all times and in all weather conditions.

IRNSS – An Indian Initiative

IRNSS is an Indian initiative. There was a felt need for an indigenous version for quite some time, but it was especially felt during the Kargil War against Pakistan in 1999. Pakistani troops had taken positions in the high mountains of the Himalayan range, and the Indian military force desperately needed the GPS data of the region in order to combat against the enemy. But USA, that owned GPS, denied its access to India. This experience at Kargil made the nation realise the importance of an indigenous navigation system. This was the beginning of the development of IRNSS by the Indian scientists in ISRO. IRNSS-A, the first of the series of satellites, was launched on 1st July 2013, and there were several other launches that followed in the subsequent years, so that currently, there are 7 satellites in orbit for India.

International Recognition of IRNSS

IRNSS gained international recognition when the International Maritime Organisation (IMO) recognised it as a component of the World-Wide Radio Navigation System (WWRNS). This happened in the 102nd meeting of the Maritime Safety Committee in November 2020, where it stated that NavIC met the operational requirements to assist in navigation of ships in ocean waters. NavIC can be utilised in such areas as maritime navigation and survey. Undoubtedly, this development is in line with India's *Atmanirbhar* (Self Reliant) initiative.

by Susan Koshy, Editor-in-Chief, with V Rajendran, Editor
Source: Dec 2020 issue of PreSense

*****

iOS (iPhone Operating System) vs Android Operating System

Millions of people globally use only smartphones as it is like a mini version of the laptop in their hands. The majority of the Smart phones are operated under Apple's iOS and Google's Android. Here we look into some basic features between iOS and Android and their differences and efficiencies.

Smartphone users globally are estimated to be 3.8 billion, and this means approximately 48.33% of the world's population owns a smartphone. China, India, and the United States of America are the countries with the highest number of smartphone users. Overall, there are around 1.65 billion Apple devices in active use. Apple counts a device as active if it has engaged with an Apple service within the past 90 days. There are over 3 billion active Android devices in use now globally.

A majority of the people uses smartphones to communicate and this is where social media plays a major role. Social media use continues to grow, with global users reaching 4.33 billion in April 2021, majority of the people find easy to connect through Smartphones instead of bulky desktops, laptops etc.

Mobile Operating System Market Share Worldwide:

iOS - 26.46% |Android - 72.72%
(Source - gs.statcounter.com)

Ease of Use

It's certainly true that the iOS interface is easy to use but can't control the system. Android smartphones gives more control over the system and its applications.

Fit, Finish and Price

iPhones are beautiful in their appearance and renowned for their firewalls against viruses corrupting the OS by user's penchant for downloads. But user will never find a "cheap" iPhone. They are pricey because of the build, finish and software, which comes from well-defined research.

Android phones — well, they vary. Wildly. The major reason for this is Android OS been used across many manufactures.

Closed vs. Open Systems

iOS is a closed system whereas Android is more open. For most users, this is the vital difference. Especially for users who want more and more apps to download on their phones, Android is comfortable.

iOS users can download iOS apps, but will not be able to download other unverified apps. Apple, the proprietary owner of this technology software, plays safe and has built very strong firewalls into its phones so that it is not corrupted by viruses from uncertified apps.

Apple has not ported any of its applications to Android. Android is both open source and far more open to alternative applications.

Voice Assistants

Apples Voice assistant named as 'Siri'. Siri may have been the first to market, but it's still pretty basic. It's fine for answering questions, but it's not really that much of an assistant. Androids Voice assistant, more popularly known as Google Assistant, is more than an excellent with voice interface to Google search. The experts say, it can make life simpler.

Timely Updates& Security

For iPhone, every detail and update is under Apple's control.

When it comes to Android, Google supplies the base operating system updated programs, and it is up to the phone manufacturer to deliver upgrades and patches. When users want to upload their Apps to Apple iOS, they have a long procedure and a dedicated team for the security of user's data and other parameters of security.

In Androids Play Store, anyone can upload their Apps and that is where the data security can be questioned. Androids Play Store also contains 'verified Apps' where those Apps are safer to use.

Peripherals

With iOS devices, users need something that will connect with its proprietary Lightning port which is also costly in Markets. Android devices use standard USB ports and Type C Cables, so there are many gadgets users can connect to their phone and also they can get these peripherals at their desired cost. Type C cables are quick to use and better compatibility with new gen phones.

Cloud Integration

iCloud continues to be a bit problematic when users try to use it apart from their iOS devices. According to discussions and reviews, a large number of people face the same issue.

When a user signs up for iCloud, he automatically gets 5GB of free storage. If he needs more space in iCloud, he has to upgrade to a larger storage plan.

Android, however, is tightly integrated with Google's applications and services. Google Photos has unlimited storage and includes a decent basic photo editor. Google Drive gives users 15 GB of free Storage.

Hardware

Hardware varies from one phone to another. Even iPhone models differ in the features they offer. But in general, the iPhone has a uniform look and parts. Since only Apple manufactures the iPhone, they get to have full control over the design.

On the other hand, Android phones look a lot more different from each other than iPhones. And the reason is that there are dozens of manufacturers from Samsung to LG who market these devices. That means some Android devices may have plastic lenses while others have glass depending on the manufacturers cost.

Well, it is quite hard to come to a conclusion which is better. But these are all the basic differences among these Operating Systems.The ecosystems of both phones have their advantages and disadvantages. In fact, phone companies, even the top ones, use both metal and plastic bodies to reduce prices to compete in the market. Though plastic body phones are vulnerable to breakages, metal ones sturdier, commonly used phones have only plastic bodies.

by Srinivas Gopal, Mobile Technology Advisor
Source: June 2021 issue of PreSense

*****

Interview with Dr Sam Pitroda, Father of Indian Telecom Revolution

"We need technology in agriculture to improve the income of our farmers"

The Editorial Team of PreSense had an interactive session with Dr Sam Pitroda, an internationally renowned telecom inventor, entrepreneur and policy maker with over 50 years of experience in the Information and Communication domain. We reproduce an extract from the interview. The recording of the full interview is available at https://www.youtube.com/watch?v=9Inz9VKDv1I .

Q1. Why is India not able to merge technology with agriculture which is the backbone of the country?

Dr. Pitroda: In agriculture, technology has a lot to do in the areas of soil, irrigation, seeds, weather forecasting, marketing, distribution and delivery. We need technology in agriculture to improve the income of our farmers. We need technology for the people at the bottom of the economic pyramid. The best brains in the world are busy solving problems of the rich. The problems of the poor do not get the right talent to resolve them.

Q2. How can we use technology with data security?

Dr. Pitroda: Technology can track you down through your credit card, your mobile phone and your social media, besides other devices. Let us accept this fact and be cautious about our private matters like health, wealth and family, where we need to keep them as private as possible. We need to take care of security here like we lock our house. We need to continuously use better locks to keep our private matters private.

Q3. Please share your experience in the technology revolution that you were involved, in the 1980s.

Dr. Pitroda: I strongly believed that connectivity could bring everyone in this diverse and interesting country together. When the then Prime Minister approved my proposal, I was empowered with the political will to do something for this country. The focus was to improve access to telephones rather than telephones themselves. The idea of STD PCOs (Public Calling Offices) booths, developed with indigenous resources, became popular. Thus, in forty years, from just 2 million telephones for which we needed to wait 10 years, India now has 1.2 billion phones.

Q4. In the banking sector, how do we maintain the right technology while maintaining high security?

Dr. Pitroda: In today's banking, transacting is almost instant to any place in the world so that distance is irrelevant and time is instant. When compared to the volume of banking transactions running to trillions and trillions every day globally, the extent of frauds is miniscule, and it is calculated into the cost of banking. And the banking sector is doing its best to take care of the threats and risks.

Q5. How do you see our education system and what would you suggest for change?

Dr. Pitroda: We need three things for education – motivation, time and content. If one has the motivation and time, content is

available on the internet. So, we do not really need a teacher in the conventional sense, but a mentor. Therefore, we need to change the education system. There are three challenges to address – expansion for inclusivity, quality of education to equip students to solve problems and not learn by rote, and reach so that the poorest of poor have access to proper education.

Education is fundamentally about being a good human being and a good citizen – a self that is disciplined, respectful, creative and comfortable with oneself. The three fundamental things in life are to love, be engaged/occupied, and be fulfilled with life.

Q6. What are the strengths you see in the Indian youth today? Do you see any area for improvement?

Dr. Pitroda: India has an advantage because of its large number of the youth. Our young people should be the workforce for the world, solving problems of the world, and not just India. We need to build their character to see beyond making money at some point. They needed to trust in life, practise truth, respect one another, heed age, experience and wisdom, and build an inclusive society.

The Team comprised Prime Point Srinivasan Managing Editor & Publisher, Susan Koshy, Editor-in-Chief, Priyadarshni Rahul, Deputy Editor, and Srinivasa Gopal, Technical Support.

by Susan Koshy, Editor-in-Chief
Source: Dec 2020 issue of PreSense

*****

Beware! Domain-Spoofing – Another Phishing Attack!

A WhatsApp message was doing the rounds, reading as under:

"Important… Spot the Difference? ***gtbank.com*** *is not the same as* ***gtbank.com,***
ecobank.com *is not the same as* ***ecobank.com.***
The first one is correct, the second one is from hackers.
The "a" in the second URL is a letter of the Cyrillic alphabet.
An average internet user can still fall for this.
Be careful for every mail requiring you to click on a link.
Please Stay Alert. Cyber-attacks have gone steps higher."

Only by careful scrutiny, will you observe the difference in the letter 'a' in both the cases. That is to say, a different font of 'a' has been used. This is an emerging *modus operandi* in phishing attack, called Unicode Domain Spoofing or Domain Name Homograph Attack or Script Spoofing.

We normally create websites, giving our names in conventional, standard and popular fonts. Thus, when we type the URL in any font, it will go to the website. On the other hand, we can also create websites (domain names) in Unicode itself in which case, at the time of creation, we will give the Unicode16 expression of our domain name and deliberately use the letters say 'a' or 'o' or 'u' or 'w' (in fact most of the letters) which are available and accepted in non-conventional format/font itself, just as we create a domain name or register a URL in Tamil or Telugu or Devanagiri-Hindi or any vernacular language.

Technologically, we use a virtual keyboard (fonts) with our normal keyboard! After creating such a website, you cannot type the URL and go to the site. You have to copy paste the URL and reach the site. For phishing type of frauds, this is quite handy. They deliberately register a domain in the name of a popular website, using a Unicode font (like creating a Tamil or other vernacular language website), and will only send you the link (and not allow or expect you to type the URL) to reach the URL. You will land on this fake website. When you actually type the URL, you may land in the original. When you paste the URL or click the link, you will land in the fake website!

Therefore, it is worth repeating a hundred times:

- Never click a link!
- Remember, malicious users and fraudsters can register fake domains that look like real website domains.
- Take pains to read the website name and type it.
- Beware!

by V. Rajendran, Editor
Soutce: April 2021 issue of PreSense

*****

Index

N

O

P

R

S

T

U

V

W