Cyber Times

An initiative towards Cyber Security...

EDITORS COLUMN

Today, we are happy to present the first edition of the newsletter. This TechNewsletter is started as a medium for displaying the departmental achievements, activities and latest news about cyber space.

It will help us to share knowledge among ourselves. We wish a long journey for this. We are thankful to administration for their kind support.

-Team Newsletter

I appreciate the initiative of students for bringing out this newsletter with the objective of creating awareness among people towards Cyber security and related domain. I wish this will be brought out on regular basis.

This newsletter will not only be useful for the students, faculty and staff of the University but also for the society in a large.

I convey my best wishes.

M.L. Kumawat
Vice Chancellor,
SPUP, Jodhpur

Edition Highlights:-

We are building our lives around our wired and wireless networks. The question is, are we ready to work together to defend them?

-FBI

Cyber Crime: Challenge to Indian Law Enforcement Agencies

Cyber Crime has become the most challenging task for our police system. Officers are facing a lot of difficulties in investigating these types of crimes. Lacs of cybercrimes have been registered under IT (Information technology) Act 2008 but only seven has convicted. So it has also impact on Indian police as well as jurisdiction.

Lack of technical capabilities

Most of the officers who investigates these cases are not technical and even they are not aware about the terms used in this environment. They mostly deny to register these cases by excusing that these cases have never been solved.

If they go on crime scene they cease the computers and all other devices as they do for conventional crimes and this destroys all the evidences against criminals.

Lack of coordination of other state's police

A cybercriminal does not bound with physical boundaries he can be anywhere around the globe. So, during the investigation police need to be interact with the police of other states to reach the criminal. But it is very difficult task to take help from other states police. The police don't have centralized database of criminals hence it make this hard to catch these criminals.

One of the main characteristics of cyber-crime is **borderless**. The perpetrator is not limited to geographical boundaries of a city, state or even country. E-frauds like 419 scams are mostly done by a racket which includes local as well as criminals from other countries so police is able to catch local persons but the master minds are never caught.

Most of the hackers traced are outside the country so the investigation is interrupted due to the lack of support by police of that country.

-Sachin Mittal
Commissioner of Police,
Jodhpur

So most of the criminals traced are from other countries like Pakistan, China and Nigeria. Hence police cannot do anything without the help of these Countries which often refuse to give the right information about the criminal so police is unable to do anything without their support if they are not forced to help by some international treaty.

Multiple jurisdictions:

Laws differ from state to state and country to country. So an act that is illegal in a region may not be crime in other jurisdiction. It becomes very typical when the perpetrator is doing act where it is not illegal but the victim comes in the jurisdiction where it is illegal.

Anonymity

It is very easy to hide the identity on internet by using proxy servers which provides you temporary IPs so it becomes very difficult to track them.

Nature of evidence

It is also the most important thing which make cyber-crime more difficult to investigate and prosecute in comparison to real world cases. Here everything is represented in form of bits (zero or one).This type of information is fragile and can be destroyed easily.

This type of information also have certain validity time. The integrity of such information is a very big issue. As Indian courts take large amount of time to make the judgment so these evidences can be easily altered or destroyed till date or the resources like hard disk, RAM which has limited time validity for data and in this case the evidences are lost. Most of the time electronic evidences are not captured properly and not preserved and presented according to Indian Evidence Act.

Some of the offences are made bailable under IT Act so after getting bail accused's primary goal is to destroy the evidences that make conviction rate very low.

Judges as well as lawyers

In the courts are also not technical so they face very much difficulty in making conclusion in these cases. Judges are fully dependent on a few lawyers who have some knowledge of IT Act and computers. So it become very serious issue to make the fair judgment for victim. They even don't know about the IP address of a computer then how we can v expect judgment from them.

The **Servers** of different service providers like Gmail, Facebook, and Twitter etc. are located outside country so when LEA (Law Enforcement Agencies) requires some information then they have to write to country representative then he writes to the concern authority to get the required details like account information.

And due to the privacy issues sometimes they refuse to give the user's information for example US also have data privacy law but India don't have.

Cases not reported

Most of the people are not aware of IT Act so after becoming victim of a cybercrime they even don't know that it is a crime and where to report it. So the law enforcement agencies have troubles in identifying these criminals and they are unable to create profile of these criminals.

-Hetram Yadav

Govt. has said in Rajyasabha that 1600 arrests have been made related to cybercrime under IT Act 2000.

The NCRB records also show that 217,288, 420,966 and 1,791 cybercrime cases were registered under IT Act, 2000 during the years 2007, 2008, 2009, 2010 and 2011.

But only 7 convictions are made till now which is very shocking.

QUIZ 1:- When senior officials of a Fortune 500 company found out that certain employees were operating internal slush funds totaling about $286 million dollars, they called in a computer forensics professional to find out why and to assess the impact.

Please explain how the computer forensics professional went about resolving the problem.

World War C

-Nishant Grover

What is it?

Our world, is about to face a new kind of war, which mankind has never seen before, The Cyber World War. "In that shadowy battlefield, victories will be fought with bits instead of bullets, malware instead of militias, and botnets instead of bombs" [Fire Eye 2013]. These assaults would be largely unseen and unheard by the public, unlike the wars of history, there won't be any exploding warheads, destroyed buildings or frightened civilians but the list of casualties will be including leaders of technology, financial services, defense and governments. A cyber-attack is not an end in itself but rather a potentially powerful means to a wide variety of political, military, and economic goals.

How it will happen?

A country's strength and defense primarily depends on its military, government and intelligence agency networks. If hacked by any other country, not only classified information may get in wrong hands, but also the network itself can be disabled and it can be further used to disable other smaller networks in the country. Once the communication and defense systems are down, a full scale military assaults can be launched which would be like slaughtering an unarmed pig. In today's world, communication is very important. It is very need for remaining up-to-date about what it is happening in the world. If it is gone, a country would be blind for the period of time. It will not only be disconnected from world but also from its own potential allies.

A soldier blinded for few seconds in battlefield dies, if you blind a country for 24 hours, the loss of life becomes unthinkable.

Is it possible for cyber-attacks to deal physical damage?

Yes, it is possible to do so. Hacking into power plant networks of country and overloading components can do real physical damage to components not only on plant but it can also spread to domestic households and industries connected to it. As a fact, world has faced it already. Iran was subjected to cyber-attacks in year of 2010, when a special malware attacked the nuclear facility in Natanz known as Stuxnet. It was believed to be a combined effort of Israel and United States although it was never proved or taken responsibility by any.

Stuxnet destroyed Tehran's 1000 nuclear centrifuges by over speeding them while making sure that sensor still showing the normal readings to operators. This set back the country's atomic program by at least two years, as it spread beyond the plant and infected over 60,000 computers as well.

Preventive measures

Although cyber war can't be prevented, yet measures can be taken to minimize the damage occurring due to it. Like Army is to defend land, Navy to defend waters and Air force to defend air space, there is a desperate need of cyber army to defend the internet boundaries of a country's networks. One Cyber army which go in hand with different departments of a country, helping them to make their network defenses stronger, enhancing intrusion detection systems and if in case a penetration occurs, analyzing it and preventing the same in future. Our World is changing rapidly, due to new technology emerging each day it is very essential to prevent the misuse of same to make the world a better place for everyone.

Need of Cyber Security

-Naresh Saini

When the life was started in Nature, the life wanted security to sustain in Nature. In this process life used god gifted behaviors. After some time the challenge's was changed according to population and many more environmental changes. So the human being required a new thing for protecting them. In this thing they developed some systems for helping them for example "arms" were using for protection against animals and they used to kill them but in night for security purpose they developed a system that is called "home" and they also use fire. It means if we want to secure against emerging security issues then the need of time is that we have to develop a new system.

After evolution we are in 21th Century where we use many technologies to secure our life and communicate to each person in any time for sharing information. Information is a very useful data for desire person. For example a person tell another person about his area condition's then the second person already aware about this area's condition without traveling that area. When we talk about information sharing us share weather situations for farmers, what happen in our social life, what happen in our country, the national and international issues and our business information etc. In this sharing and communicating process we use many devices like cellphone, pc's, tablets etc. These devices are available in market at very low cost. So every person can afford these devices that are connected with network. In these devices many kind of applications are used for connecting each other and share information on social network like Facebook, twitter, LinkedIn, Instagram etc. And for personal data sharing used whats app, viber, wechat line etc. We share our information like photos, videos, id's, banking details (for business purpose), personal details etc. on a network.

The gadgets and applications have been changed every person's life. So, in these days many persons are fully depending on these devices and applications. They use it to send & receive any kind of information. It may be personal, social, national and international. Every person in the world is using and also depends on them. It means every person who wants to know about any other person that is on networks can gather his information in very short period of time. So this type of communication system is possible in "cyber system".

About the cyber system we can say it is a powerful system for a person, organization and a country etc. But the every system has both advantages and disadvantages. In the cyber world there is a possibility that personal data may be theft by third person and misused by that person. In an organization , the organization have secrete data for their own business if this type of data are leaked on a network by any means it's very harmful for this organization and it may be possible that the organization is totally takeover and can be destroyed. If a third party or a person hacked a country's sensitive data like control of energy resources, security aspects , trade information's , market policies , economical information's and many more important data of a country then it means the country's control system will totally go into the third party's hand. It means other country can easily destroy that countries energy resource, economical infrastructure, markets. In personal way every person uses cellphone it means if an illegitimate person knows about cellphone's weakness then he can use your cellphone to spy on you. Means he can knows about your address, your location , your personal information like user id, password, bank details etc. and this information can be used for theft, kidnaping, sharing your id for illegal activities like transfer money from your account to other account

etc. It's all do from a different region, different country by pressing some keys of a computer and using network connectivity. It means if we connect a network then we are not secure any time so we are in risk. Many countries make some expert to analysis this network to make it secure and improve these benefits. These experts are called "cyber experts".
But in India there are few cyber experts which are not sufficient .It means we are not secure from other country cyber-attacks, but in few time we are worrying about these type of security and establish many universities in India for making cyber experts. In this way the SARDAR PATEL UNIVERSITY OF POLICE SECURITY AND CRIMINAL JUSTICE is first that will provide cyber experts to India from 2015.

Hack Trick

These tricks will improve the speed & load time of Firefox. And you will be able to surf faster.
Type **about:config** in the address bar, Than look for the following entries, and make the corresponding changes.

1. network.http.max-connections-per-server =32
2. network.http.max-persistent-connections-per-proxy =16
3. network.http.max-connections = 64
4. network.http.max-persistent-connections-per-server = 10
5. network.http.pipelining = true
6. network.http.pipelining.maxrequests = 200
7. network.http.request.max-start-delay = 0
8. network.http.proxy.pipelining = true
9. network.http.proxy.version = 1.0

Lastly right-click anywhere and select New- Integer. Name **itnglayout.initialpaint.delay** and set its value to 0. This value is the amount of time the browser waits before it acts on information it receives. Enjoy!!

Contributed By: Yogendra Singh Chahar

Real Time Case Study: Cyber Crime Case Solved by Gurgaon Police

Genpact BPO Case

A complained was registered by Mr. Vikas, G.M. H.R. of Genpact . It was mentioned that some unknown person is sending obscene mails to female staff working at the organization.

- **IO asked the complainant for email copy along with email header.**
- **After receiving the above header copy he checked for the IP address mentioned in the header part**
- **Once he found the ISP's name he sent notice to the ISP to provide the IP address detail**
- **He got the email address which was used by the accused to send mails and it was found to be from rediffmail.com.**
- **Then a notice was sent to the rediffmail.com to provide login, account creation and password change IP details.**
- **He received all the IP details from ISP and checked it at the APNIC site and found that its from the same ISP i.e. Airtel.**
- **He received IP address detail from ISP, and it was done from a cyber café at Dwarka, Delhi.**
- **The cyber café guy was called-up to verify the given IP address details.**
- **Then he checked the register maintained by the cyber café owner and found the guy using internet. He got the phone number and name of the accused person.**
- **They called-up complainant to check their employee database and provide us those names who are residing at Dwarka, also asked them to check those who left the organization within a period of last 3-4 months.**

The above case was traced and the accused was found to be an employee of the complainant organization.

IT Act applicable:

66A: Punishment: imprisonment up to 3 years with fine.

Sec 67,67A: Punishment: imprisonment up to 3 years with fine up to 5 lakh rupees and in the event of second conviction with imprisonment for a term which may extend to 5 years and also with fine which may extend to 10 lakh rupees.

Compiled By: Hetram Yadav

QUIZ: 2

Suppose you are an investigating officer and found an account to be used for uploading offensive messages. You want to delete that account permanently (not deactivate) so that it cannot be activated again. What is the link? (Assume that you have password)

Security Issue with Android Smartphones

By: - Vikas Yadav

Today Android is well known name in mobile Operating System which is based on Linux kernel that is currently developed by Google. According to a survey 80% mobile devices are running on Android.
Android is designed primarily for touchscreen mobile devices such as smartphones and tablet computers, with specialized user interfaces for televisions like Android TV, cars like Android Auto and wrist watches. Google acquired Android on August 17, 2005. The first commercially available smartphone running on Android was the HTC Dream, released on October 22, 2008. In 2010, Google launched its Nexus series of devices. But here question is that android is secure or not about smartphones users information. Study says that most of the mobile apps are not secured.
Research from app development firm RIIS (Research into Internet Systems) claims mobile apps from big brand name like Walmart and Delta, are full of security loop-holes that can expose sensitive information. In a study on mobile application and their level of security RIIS, LLC, a firm that is well known in mobile app development, said that some of the nation's top brands, including airlines, retail outlets, entertainment companies, and insurance companies, are developing applications for Android that place users and their personal information at risk.

TOP 10 Mobile Security Risks

Today, in the digital world everyone is now connected to internet via smartphone. This extreme level of convenience has brought with it an extreme number of security risks across the net.
Here I'm discussing top 10 mobile security risks.

1. Insecure Data Storage

Insecure data storage can result in data loss for a user. One who loses their phone, or for multiple users if an app are improperly secured, leaving all users at risk.
Data that are stored and potentially at risk:

- Usernames
- Authentication tokens
- Passwords, Cookies, Location data
- EMEI, Device Name , Network Connection Name
- Personal Information like DoB, Address, Social, Credit Card Data
- Application log files and browser history

2. Weak Server Side Controls

This risk is quite simple. The servers that your app is accessing should have security measures in place to prevent unauthorized users from accessing data. This includes your own servers, and the servers of any third-party systems your app is accessing.

3. Insufficient Transport Layer Protection

When designing a mobile application, commonly data is exchanged in a client-server fashion. Data is exchanged across the internet. If the application is not properly coded, and not secured, "threat agents" can use techniques to view sensitive data while it's traveling. Agent can compromise or monitor network.

4. Client Side Injection

Android applications are downloaded and run on "client side". This means that the code for the app actually resides on the user's device. Attackers can load simple text-based attacks that exploit the syntax of the targeted interpreter.

5. Poor Authorization and Authentication

Apps and the systems they connect should be properly protected with authorization and authentication best practices. This ensures that devices are authorized to transfer data and that unauthorized devices are identified and blocked.

6. Improper Session Handling

Have you ever been in the middle of checking your bank account online when your attention is called away? You return to your computer to see a message like, "Session Timed Out - Please Login Again". This is an example of a session handling best practice. You were inactive for a determined amount of time, and the system logged you out. This prevents threats like someone from sitting down at your computer and seeing your bank account**.**

7. Security Decisions via Untrusted Inputs

You might assume that inputs such as cookies, environment variables, and hidden form fields cannot be modified. However, an attacker could change these inputs using customized clients or other attacks. This change might not be detected so attackers can bypass the security of the apps.

8. Side Channel Data Leakage

In cryptography – the strategies used in encrypting code, a side channel attack is any attack based on information gained from the physical implementation of an encryption system, rather than attacks through brute force or theoretical weaknesses in the algorithms. Watching how, when and where the data moves, attackers can find and exploit security holes.

9. Broken Cryptography

Encryption systems are constantly evolving. Ensure that the cryptographic technique you are applying is stable and has not been broken yet. This weakness can be detected using tools and techniques that require manual human analysis, such as penetration testing, threat modeling, and interactive tools.

10. Sensitive Information Disclosure

Though listed last, this is one of the most severe points of vulnerability in mobile app security – because it's out of your control. When apps, systems and cryptography created or used by other companies are hacked or broken, your data would be at risk. Once these pieces of sensitive data have been disclosed, they can be used to mine other databases and systems for access to accounts, credit cards, usernames and passwords and more.

References

[1] https://www.riis.com/
[2] https://www.android.com/

Need of Policy to Stop Job Scams

Balram Choudhary

Recently as increase in population and education simultaneously crimes over internet increased rapidly. One of the most important crimes is cheating peoples by playing with their needs and the most important need for an educated person is to get a job. When someone is seeking for job and if he is unable to get job then he tries every single advertisement that are placed and these all can leads him to some fake job vacancies too. These fake job vacancies are the medium for getting money without any trouble (until there is no legal framework for this). Some poplar job advertisement sites are also path for scammer's until and unless we ban or restrict them to do so.

1. Loss due to these scam/ fraud

a) Identity of applying persons is being theft and this can cause serious long time harms to that particular person. His identity theft involves date of birth, social security number, Aadhar card, voter ID card, gas connection number, pan card, bank a/c number, educational qualification, marital status, email id, number of family members and a lot more. Everything is in wrong hands just because you are applying for a job.

b) Further this data can be sold to anonymous and private organizations looking for sell of their product and advertising. There will be a lot of calls related to your profession for jobs, products, services, home appliances etc.

c) Identity can be used for other person with the help of duplicate documentation of every single document. For example they have every single document, photo, signature and personal details and these all are enough for buying a new SIM. This can be used by terrorists too.

d) First people pay for application form then for call letter they can also say that you have to deposit this amount of money for your next step of recruitment. Thus People pay a lot of money to these kinds of firms. The time involved for the process of job application to knowing that it was a scam is total wastage of human resources of this country. Peoples are being harassed due to money laundering and time wastage involved in all these..

(e) Applying persons are losing their faith and trust with respect to jobs. One side, we are proud of having so much young talent all around the world and another side we are just not able enough to give them trusted employment. It also increases the number of educated persons which are going towards wrong way and doing something that is not desirable.

2. Prevention techniques

Every organization who wants to give an advertisement of job vacancy should follow the following (if there is any legal work done related to below written then it should be imposed as quickly as possible and if it is not then there should be some policy work for this)

- It should have a RBI approved bank account. Here I mean that government should have a policy about this approved bank account. Bank accounts those which are used in job application form fee and advance deposit should be functional within a criteria defined by RBI and RBI should have a trail for every accounts movement.
- Government should have a separate server for job advertisements that can be run by charging a fix charge for giving job advertisement. It will also generate a fixed revenue and control to overcome cybercrimes.
- Every organization should have the physical assets equal to the money it is going to have by submission of form and bonds, fee etc. It will help us to control cybercrime involved in job scams because if any company does a job scam then through its assets we can recover money involved in it.
- There should be a separate department that will always have an eye on each and every job advertisement. This department will check for physical assets and genuineness of that particular company.
- Websites showing such advertisement should be functional within finite criteria; so that it will be easy to stop scammer's having his scam job advertisement on popular employment websites.
- Control over these all will also reduce data load over cyber space and it will be easy to aware peoples about all these kind of scams.

Warning: Don't Run These Commands On Linux, Ever!

Linux's terminal commands are undoubtedly very useful. The fact that Linux won't ask you for confirmation if you run a command that won't break your system makes online trolls into luring you into running some not so very useful, but dangerous commands.

1. rm -rf /
Deletes everything including files on your hard drive and files on connected removable media devices.

2. :(){ :|: & };:
This bash command is actually a denial-of-service attack. It defines a shell function that creates new copies of itself that continually replicates itself quickly taking up all your CPU time and memory causing your computer to freeze.

3. mkfs.ext4 /dev/sda1
Equivalent to running format c: on Windows.
mkfs.ext4 – Create a new ext4 file system on the following device.
/dev/sda1 – Specifies the first partition on the first hard drive, which is probably in use.

Compiled By: Vikas Yadav

"Everybody is a genius. But if you judge a fish by its ability to climb a tree, it will live its whole life believing that it is stupid."

-Albert Einstein

A Help desk guy speaking to a lady user...

Help desk: Double click on "My Computer".

Lady: I can't see your computer...

Help desk: No...Click on "My Computer" on your computer.

Lady: How the hell can I click on ur computer from my computer???!!

Help desk: there is an icon labeled "My Computer" on your computer... double clicks on it...

Lady: What the hell is your computer doing on my computer??!!!

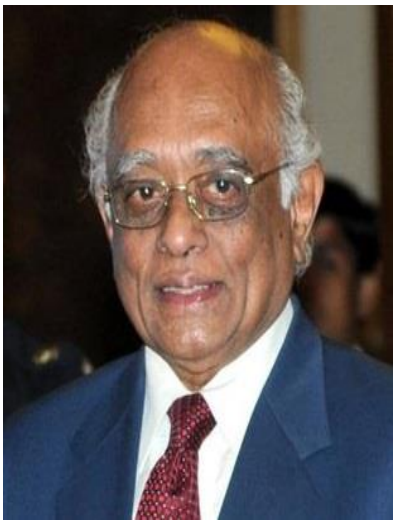
QUIZ 3: Stuxnet has been called a "digital super weapon" apparently intended to:

A. delete Bill Gates's bank account information
B. delete Wall Street financial data
C. wreck Iranian nuclear centrifuges
D. cause a blackout of the US power grid

Personality Profile

Dr. Rajagopala Chidambaram

Principal scientific advisor Government of India



Name: - Dr. Rajagopala Chidambaram

Year of birth: - 1936

Specialization: -

Material Science and Crystallography, High Pressure
Physics and nuclear technology.
Played a key role in the 1974 nuclear explosion experiment at Pokaran and led the Department of Atomic energy (DAE) team in the Pokharan-II tests in May 1998. His Key participation in the design and successful execution of operation smiling buddha saw him leading the DAE team of operation Shakti in 1998.

Educational Qualification: -

Ph.D., DSc (IISc), DSc.

Dr. Chidambaram completed his B.Sc. (Hons.) in Physics at and M.Sc. in Physics with the specialization in analogue computers at University of Madras. He completed his Ph.D. in nuclear physics, at the Indian Institute of Science, Bangalore. His Ph.D., research thesis on Nuclear Magnetic Resonance was awarded the Martin Forster Medal for the best Ph.D. thesis submitted to the IISc during 1961-62. He was also awarded the D.Sc. in Metallurgy and in material science, degree by eight Universities.

Awards and honors: -

Padma Shri (1975)
Anand J.L. Nehru birth centenary visiting fellowship (1992)
Indian science congress (1995)
CV Raman birth centenary award of IISc (1995)
R.D. Birla award of the Indian Physics association (1996)
Padma Vibhushan (1999)
Meghnad Saha medal of INSA (2002)
Homi Bhabha lifetime achievement award of Indian nuclear
Society (2006)
Lifetime contribution award (2009)

Institutions and memberships:-

Chairman: - Scientific advisory committee to the cabinet
Board of Governors of IIT Madras
High level committee for establishing the Integrated National knowledge network

Chancellor: - University of Hyderabad

President: - Sree Chitra Tirunal Institute for medical sciences and technology, Trivandrum

Fellowship: - All the major science academies in India as well as the academy of Sciences for the Developing world (TWAS) Trieste, Italy

Membership: - Prime minister's council on climate change

Compiled By: Nitish Vyas

QUIZ 4: Which Tom Clancy novel title includes the two-word-phrase name given to a global cyber espionage network uncovered by Kaspersky, the Moscow-based anti-virus company that claims it was created by someone with "Russian-speaking" origins?

A. Hunt for Red October
B. Red Storm Rising
C. Red Rabbit
D. Threat Vector

Departmental News:

Workshop, conferences and seminars attended

(1) Cocoon 2013- International conference on cyber security (28th-29th September 2013)
(2) Delhi Cyfy - Cyber security and Cyber governance(15th-16th October 2013)
(3) NIT Warangal- Advance wireless and mobile network technology(3rd -7th October 2013)
(4) CERT-IN Delhi Workshop on Cyber security and Cyber forensic (18th -19th December 2013)
(5) RPA Jaipur -5th Cyber Crime awareness workshop for law enforcement agencies(12th-13th February 2014)
(6) Jindal Global University- The information society challenges for India (7th-8th June 2014)

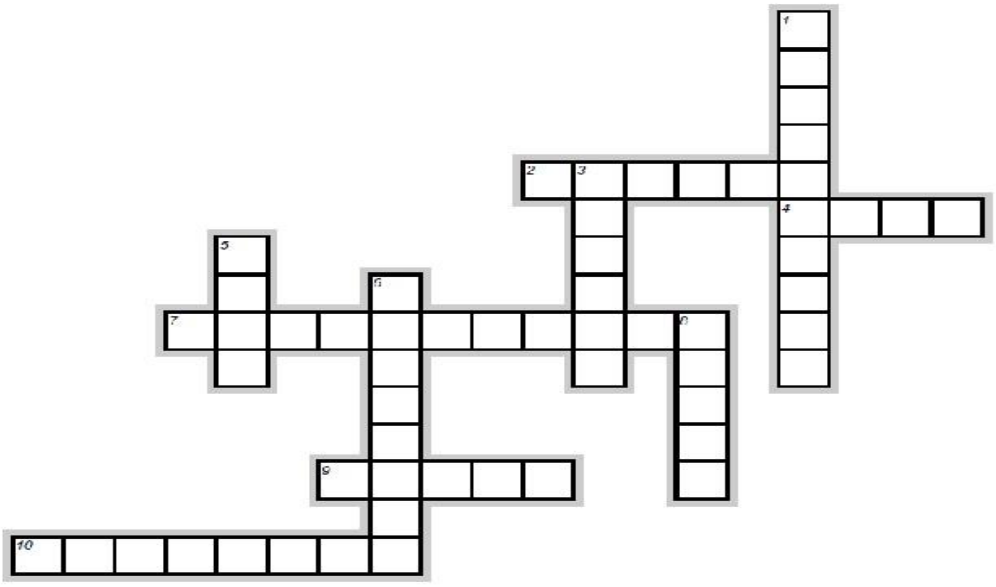
VC & Student with NTRO Director at Jindal Global University, Sonipat

Call for articles:

Students are invited to get involved in the TechNewsletter activities by providing articles and other related materials. Suggestions and feedbacks for the improvement of the newsletter are most welcome and contributions are invited from the faculty and students of the department. Contributions can be from any of the whole gamut of activities in the department like any special achievement, an admirable project, a publication, and Cyber Crime case, Quiz, puzzles or even the fun section material like jokes, cartoons, interesting facts or poems. You can also report any interesting workshops or talks taking place in the department.

You can send your material on: - **editors@policeuniversity.ac.in** by 10 September 2014.

CyberSec Puzzle



Across

2. A person who breaks into computer to view and possibly change information they shouldn't access
4. Short for "web-log", a personal web site that is usually used to keep a journal or diary
7. A harmful software program in disguise
9. A browser window that appears on top of another window, often show advertisements
10. Getting information from a computer somewhere on the internet and transferring it to your computer.

Down

1. Using the internet to harass, intimidate, embarrass, or demean others
3. A software program that makes advertisements appear on your screen
5. A harmful software program that makes copies of itself and spreads
6. A secret series of letters or numbers that you use to get access to a computer or network
8. Electronic mail that is sent over the internet

Contributed By: Yogendra Singh Chahar

QUIZ 5: Ralph Langner, the first cyber security researcher to identify Stuxnet true purpose, told the Monitor that Stuxnet represents a future in which...

A. "Everyone can be a part-time hacker."

B. "Everyone can have their own cyber weapon."

C. "Everyone will need their own digital fallout shelter."

D. "Everyone will need a digital identity card."

Editorial Board:

Hetram Yadav

Nitish Vyas

Vikas Yadav

Pragya Johari

Please send the answers of quiz and crossword on editors@policeuniversity.ac.in till 31 August, 2014. The winner will be declared on the basis of first come first serve with right answers.

The name of the winners and answers will be published in the next edition.

Note:- If any of the article is found to be copied, the writer himself/herself will be responsible for copyright issues. Editor or University will not be liable for any of the issues.

Knowledge Is Power

Brought out by the Department of Computer Science & Cyber Security

Sardar Patel University of Police, Security & Criminal Justice, Jodhpur