

The Cyber Time

An initiation towards cyber security...

Editorial

Welcome To another Issue of *The Cyber Time*

That's right, folks. The Cyber Time is six months old this month. Incredible! Never, when I started Newsletter all those months ago, did I imagine that it would still be going strong six months later. I can't stress enough that every issue is created by a team of folks, not just me, so a BIG thanks to all of them. Their names are listed with their article. I am very thankful to University administration as well as Department of Cyber Security for supporting us. I am also thankful to readers for their valuable feedback and well wishes.

I wish you very Joyful Happy New Year.

Anyway, I shan't keep you any longer. Enjoy the issue, and please send your Article and Quiz Answer!

All the best, and keep in touch!

Vikas Yadav

spu1411228@policeuniversity.ac.in

Highlights

- ❖ *Introduction of The Centre for Cyber Security*
- ❖ *National Workshop on "Cyber Security, Cyber Conflicts and Our Critical Infrastructure"*
- ❖ *UK is seriously worried about Cyber Crime*
- ❖ *HeartBleed*
- ❖ *Open proxy server*
- ❖ *Microsoft warns of Windows zero-day-hackers serve exploits in PowerPoint files*
- ❖ *Personality Profile: Mark Zuckerberg*
- ❖ *Google Changes Its Search Algorithm to Fight Piracy*
- ❖ *Google Offers Physical USB Security Key*
- ❖ *Cyber Tech Cross Word Puzzle*
- ❖ *Departmental News*

SPUP Introduces Cyber Center and National Workshop on "Cyber Security, Cyber Conflicts and Our Critical Infrastructure"

Centre for Cyber security at Sardar Patel University of Police at Jodhpur has been set up with the basic aim to develop into a center of excellence in the area of cyber security. The Centre for Cyber Security was inaugurated by **(Prof.) Dr. CVR Murty, Director IIT Jodhpur.**



Photo Credit- Arjun Suthar

National Workshop on "Cyber Security, Cyber Conflicts and Our Critical Infrastructure"

Department of Cyber Security organized a National Workshop on "Cyber Security, Cyber Conflicts and Our Critical Infrastructure" from 13-14th DEC 2014. The Workshop was sponsored by Truth Labs and supported by Microsoft India. Major areas covered in workshop are IT Adoption in Law Enforcement Agencies, Cyber Attacks, Cyber Crime, Critical Infrastructure protection, Banking Technology, Intellectual Property Rights. Different professional attended the workshop from multiple fields like Academics, Govt. Officials, Independent Consultants, and Security Advisors etc. The workshop was ended with a panel discussion to planning to meet the challenges. It was the first effort of the center towards its goal. Mr. S.K. Pandey (IPS) Director of center for Cyber Security gave a deep insight of the further planning's of Centre. He told that the center is planning to give different services like Cyber Forensics, services to state Gov. of Rajasthan in Cyber Security, Hardware Testing and Policy Making etc.

UK is seriously worried about cyber crime

-Pragya Johari

Many UK citizens have become victims of cybercrime, including identity theft, hacking or abuse on social media. The losses of the country from online fraud exceeded £670 million per year (this is given that many cases go unreported), with the true cost likely to be much higher.



According to the recent research, where over 2,000 people were surveyed, more than 50% of them said they had been a victim of online crime. This category included online-based fraud, ID theft, and hacking and Internet abuse. Of those, a half also said they felt violated by their ordeal. In the meantime, the same research shows that only less than 1/3 of the cybercrime victims had reported the

incident. Almost 50% of those affected had no idea who to report an online crime to. However, the experts say this figure is expected to fall as a result of the ongoing work of the national fraud reporting center. The good thing is that UK citizens who had suffered cybercrime admitted that such experience had shocked them into changing their behavior for the better. For example, almost 50% of them immediately changed their passwords for stronger ones and 42% said they became more vigilant when shopping online.

The statistics showed that for the United Kingdom as a whole, over £670 million was lost to the ten most common online frauds within the last 12 months. These figures show how serious a toll cybercrime can take. This has been no more apparent than in the last weeks, when large-scale personal photo leaks of celebrities happened. Unfortunately, as our lives move to the online world, this is becoming more common.

The security experts explain that people can all take

simple steps to protect themselves by such simple ways as putting a password on computers or mobile devices, forgetting about clicking on a link received from an unknown sender and always logging off from an account or website.

As for people who still do not know who to report cybercrime to, the UK authorities remind that if you think you have been a victim of online economic fraud (if you have lost money), you can report it to the organization called Action Fraud – online or by phone. Victims of online abuse or harassment can report it to their local police force. It is also recommended to read general advice on how to stay safe online at getsafeonline.org.

HeartBleed

-Vikas Yadav

HeartBleed vulnerability potentially allows attackers to access confidential data within the memory space of service and application using vulnerable versions of OpenSSL.

HeartBleed is a software bug that exists on specific

servers, router, firewalls and some other devices on the Internet software called OpenSSL. It's not currently thought to be a malicious exploit that was deliberately embedded in the software when it was written or modified, but instead a bug that existed and was recently discovered. It is expected that it has been in existence in the software for about 2 years. The Bug allows an attacker of that particular server to gain access to passwords, username, private information, and encryption keys that server contains in its memory. The nature of the bug allows the attacker to do this with a significantly reduced risk of being detected, which opens up the numbers of attacker who could exploit this. The bug is estimated to exist on tens of thousands of servers on the internet, from small web shops to large enterprises. There is a patch in droves in the last two days since the announcement of the bug.

How HeartBleed Works??

It is not a problem with the TLS/SSL (Transport Layers Security Protocols) technologies that encrypt the Internet, neither with how OpenSSL works. It is just a dumb coding mistake. Using Heartbeats extension two

computers make sure the other is still alive by sending data back and forth to each other. The client/user send its heartbeat to the servers/website, and the server hands it right back. If by chance anyone of them goes down during the transaction, the other one will know using heartbeat sync mechanism.

When that heartbeat is sent, a small amount of the server's short-term memory of about 64 kilobytes comes in reply from servers and an attacker is supposed to grab it that can leak sensitive data such as message contents, user credentials, session keys and server private keys. By sending HeartBleed request multiple times, an attacker is able to fetch more memory contents from the servers. This means, everything and anything in the memory such as SSL private keys, user keys used for your usernames and passwords, instant messages, emails and business critical documents and communication, and many more is vulnerable to cyber criminals. At this phase, you have to assume that it is all compromised.

About two-thirds of web servers rely on OpenSSL, means the information passing through hundreds of thousands of websites could be vulnerable. So far Security

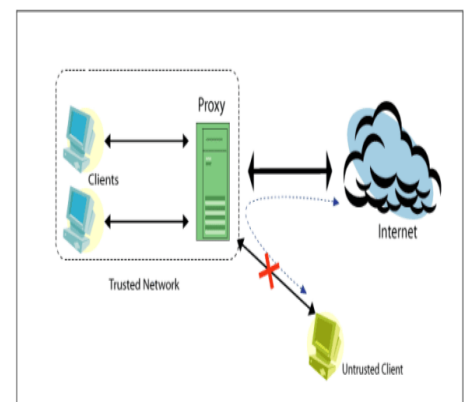
experts have found no direct evidence that anyone has managed to use the bug to steal information. The vulnerability has been fixed in OpenSSL v1.0.1g.

Major Websites, including Gmail and YouTube, Facebook, Tumblr, Yahoo and Dropbox have fixed the problem, but there are still thousands of websites who are yet to fix the problem. Users are advised to change their password on only those affected websites, that tell you they have fixed the problem.

Open proxy server

-Sashant Gaur

A proxy server acts as an intermediary between a client computer and the Internet serving as a buffer between the client computer and the Internet resources one is accessing.



When a client makes a request for an Internet resource through a proxy server, the proxy makes a connection to the requested resource on the client's behalf to get the resource and delivers it down to the client. By this process, it is able to hide the internal address of the client to the Internet and the IP address of the proxy only becomes visible on the Internet.

A Proxy Server can be used to enforce security, administrative control, and caching. A normal Web browser must be configured to use the proxy either manually or with a configuration script. A transparent proxy combines a proxy server with NAT so that connections are routed into the proxy without client-side configuration.

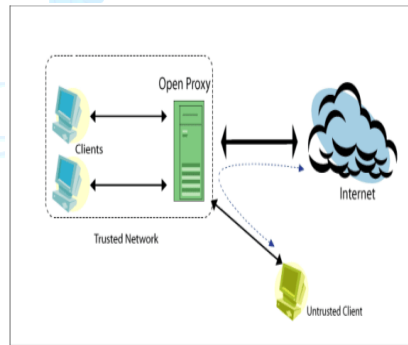
Proxies usually operate on the following ports ranges:

80, 81, 8000, 8080 (HTTPCONNECT), 1080 (SOCKS), 3128 (Wingate/Squid), 6588 (AnalogX). However, other ports can be used for the same purposes but are less common.

What is an Open Proxy Server?

A Proxy Server should accept requests from only its own clients by either forcing

a client to connect from a range of IP addresses, or by using authentication.



Any proxy server that doesn't restrict its client base to its own set of clients and allows any other client to connect to it, is known as an open proxy. An open proxy will accept client connections from any IP address and make connections to any internet resource. OpenProxy Servers act as blind intermediary to any other network addresses.

An Open Proxy Server commonly allows HTTP access but it can also be used for ftp, Usenet, email (including spam), IRC/instant messaging or even launch a DoS attack. The project Abuse-Proxy [Re:1] which aims to clean the internet of mis-configured proxy servers, maintains a database with information gathered from logs of proxy scanners run on some IRC networks. In the year 2002, 2, 80,000 open-proxies were

found in approximately 1 billion scans.

Exploitation of Open Proxy Servers

A malicious user can effectively hide his own IP address by using an Open Proxy Server for illegal activities like hacking. In such scenario instead of the IP address of the attacker appearing in the log files of the attacked system, the IP address of the OpenProxy Server shall appear. Malicious users routinely chain through several such OpenProxy Servers making it difficult to trace back to the origin of the user.

Though, Open Proxy Servers are not the same as open SMTP relays, they are infact a far more serious problem, since they allow traffic for virtually any network service to be bounced/ tunneled through the host.

An Open Proxy Server can be used by a spammer as a spam conduit to anonymously send out spam, using the resources of the owner of the proxy.

Consequences of Open Proxy Servers

An Open Proxy Server in an organization can lead to-

- The IP of the organization being blacklisted by various bodies
- The loss of image of the organization, if misused for illegal activities.
- Legal ramifications, if misused for illegal activities
- Loss of bandwidth
- It may also serve as a conduit for inbound attacks, completely bypassing a site's firewall architecture.
- It may also result in an increased risk of that host (and its network) getting scanned for other vulnerabilities

Microsoft warns of Windows zero-day-hackers serve exploits in PowerPoint files

-News

Microsoft on Tuesday warned Windows users that cyber criminals are exploiting a zero-day vulnerability using malicious PowerPoint documents sent as email attachments.

In an advisory, Microsoft outlined the bug and provided a one-click tool from its "Fixit" line that customers can use to protect

their PCs until a patch is available.

Although Microsoft does not label its advisories with the same four-step threat scoring system it uses for security updates, it said that a successful exploit would let hackers hijack the PC so that they could, for example, steal information or plant other malware on the machine.

The vulnerability affects all versions of Windows, from the aging Windows Vista to the very newest Windows 8.1, and is within the operating system's code that handles OLE (object linking and embedding) objects. OLE is most commonly used by Microsoft Office for embedding data from an Excel spreadsheet in, say, a Word document.

"At this time, we are aware of limited, targeted attacks that attempt to exploit the vulnerability through Microsoft PowerPoint," the advisory said. Other Office file types, however, could also be used to exploit the flaw.

Ironically, Microsoft patched a similar vulnerability last week when it issued eight updates, including one that

addressed a bug in OLE which, like Tuesday's revelation, had been exploited in the wild before a patch was pushed to customers.

That update was designated MS14-060 by Microsoft, and was also being exploited using malformed PowerPoint files.

According to researchers at iSight Partners, the flaw fixed by MS14-060 had been used by a Russian hacker crew to target Ukrainian government agencies, NATO, Western European government agencies and companies in the telecommunications and energy sectors, since at least December 2013. iSight slapped the moniker "Sandworm" on the cyber-spy gang.

While iSight got the credit for finding the OLE vulnerability Microsoft patched last week, a trio of Google security engineers and a pair from McAfee Security reported the latest bug.

Microsoft did not explicitly promise to patch the zero-day, but it certainly will. The only question is when. Its next regularly-scheduled Patch Tuesday is Nov. 11, or three weeks from today.

Historically, Microsoft has been hesitant to issue an emergency security update unless attack have spread widely and affected large numbers of customers.

In the meantime, Microsoft has crafted a Fixit tool that, if applied, blocks the attacks see so far. The tool is located on this support page.

Microsoft also urged Windows users to pay

attention to the User Account Control (UAC) pop-ups, the small alerts that require authorization before the OS is allowed to perform certain chores, like downloading files or running software.

UAC, which many Windows users see as an inconvenience -- and many habitually click through without a second thought -- will detect the malformed

PowerPoint file and not run its hidden malware without permission.

"In observed attacks, User Account Control (UAC) displays a consent prompt or an elevation prompt, depending on the privileges of the current user, before a file containing the exploit is executed," Microsoft's advisory said.

Q.1 First screen to appear after logging into Administration Panel of a website is known as?

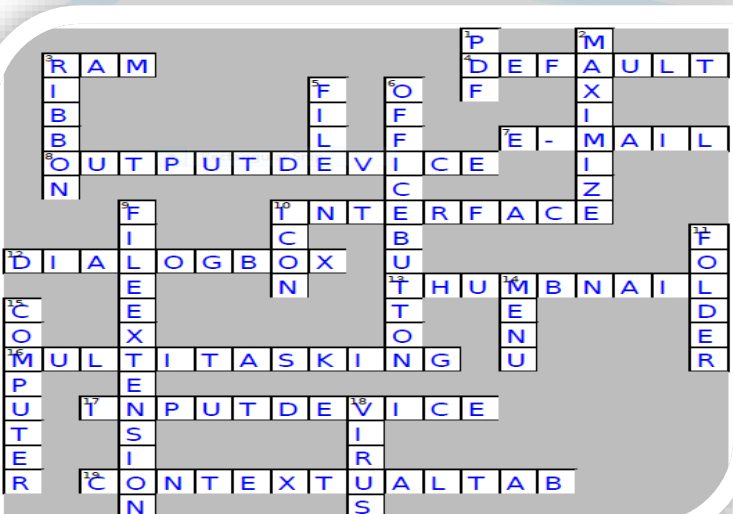
- a)Index page
- b)Dashboard
- c)Admin area
- d)Summary Page

Q.2 Adobe's most popular application for multimedia and vector animation on websites

- a)Adobe Reader
- b)Adobe Flash
- c)Adobe Photoshop
- d)Adobe after Effects

Contributed By: Nishant Grover

Previous Quiz winner



Nishant Grover

Personality Profile: Mark Zuckerberg



Mark Elliot Zuckerberg (born May 14, 1984) is an American computer programmer and Internet entrepreneur. He is best known as one of five co-founders of the social networking website Facebook.

As of April 2013, Zuckerberg is the chairman and chief executive of Facebook, Inc. and his personal wealth, as of July 2014, is estimated to be \$33.1 billion. Mark Zuckerberg receives a one-dollar salary as CEO of Facebook.

Together with his college roommates and fellow Harvard University students Eduardo Saverin, Andrew McCollum, Dustin Moskowitz, and Chris Hughes, Zuckerberg launched Facebook from Harvard's dormitory rooms. The group then introduced Facebook onto other campuses nationwide and moved to Palo Alto, California shortly afterwards. In 2007, at the age of 23, Zuckerberg became a billionaire as a result of Facebook's success. The number of Facebook users worldwide reached a total of one billion in 2012. Zuckerberg was involved in various legal disputes that were initiated by others in the group, who claimed a share of the company based upon their involvement during the development phase of Facebook.

Since 2010, Time magazine has named Zuckerberg among the 100 wealthiest and most influential people in the world as a part of its Person of the Year distinction. In 2011, Zuckerberg ranked first on the list of the "Most Influential Jews in the World" by The Jerusalem Post and has since topped the list every year as of 2013. Zuckerberg was played by actor Jesse Eisenberg in the 2010 film *The Social Network*, in which the rise of Facebook is portrayed.

Mark Zuckerberg was a Harvard freshman with a gift for computer programming. Less than a decade later, he is the baby-faced, multi-billionaire, power broker who rubbed shoulders with the President. He transformed a dorm-room project into the internet's biggest global village. The site now has over 900 million users. But for all that success, Zuckerberg has confronted bitter battles and lawsuits over Facebook's origin. He has waged an all-out war on his biggest competitors.

Zuckerberg has come under fire for pushing the limits on user privacy. He is not dealing with just a piece of technology, he is dealing with people and their behavior and in many ways he is doing it on the fly. They have humongous database of information about us because we trusted them, so the question is should we still trust them? We think we know Mark because we have seen his life unfold in the Oscar winning movie, *The Social Network*. The portrait was unsparing. A super geek, intense, cut throat, brilliant and socially crippled. But was it accurate?

Mark's mission from the beginning was about connecting people and it was clearly based on this theory that if the world were more connected it would be a better place. But there are lots of surprises when you really dig deep

into the story of Facebook. The biggest single surprise is the peculiar and tenacious personality of Mark Zuckerberg and the depth of his convictions and his consistency.

Born in 1984, he grew up in the Hudson River town of Dobbs Ferry, a bedroom community north of New York City. David Kirkpatrick spent two years researching a book about Zuckerberg and Facebook called *The Facebook Effect*. He comes from an unbelievably supportive family in which he is the only son and he has three sisters. This is a guy without any problem of self-confidence.

Computer savvy from the start, Zuckerberg taught him the complicated computer language C++ and by ninth grade had created a digital version of the board game 'Risk'. He actually created a thing called Zucknet which is an internal instant messaging system for the family so the computers could talk to each other. That's kind of a kid he was. When he got sort of tired of his local high school, he decided to go to Exeter Prep School really because he just wanted more challenge. It was at the exclusive Exeter academy that Zuckerberg and his friend Adam D'Angelo created a music website called Synapse.

Google Changes Its Search Algorithm to Fight Piracy

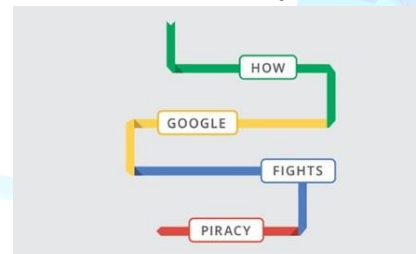
- Nitish Vyas

Google is going to introduce some changes in its search engine. They are supposed to make sure that some of the piracy services are less likely to appear in the results of searches for music, movies and other copyright material. This is not the first time the search giant was going to change the way it targets piracy.

Two years ago Google made the similar promise, which has since proved controversial. Entertainment industries were regularly claiming that Google did not follow through on that promise. Now the company says the results will be noticeable. Google explained that it has now refined the signal in ways it expects to visibly affect the rankings of some of the illegal websites. However, the tech giant didn't provide details on which websites were being demoted, or how it will affect their rankings. Apparently, the attribute showing how close to the top of its results a website appears when relevant keywords are searched.

In addition, the company claimed that it has been testing new ad formats which show links to legitimate digital music and video services when such keywords as "download", "free" and "watch" are used; as well as removing terms from its autocomplete feature in the case when they "return results with many DMCA demoted websites".

Google provided some statistics, saying that it had received just over 224 million



takedown requests for search results last year, and the average time spent on dealing with them was less than 6 hours. The tech giant ultimately removed 222 million links, which means that only less than 1% was rejected or reinstated after review for various reasons: for example, because the company needed additional information, was unable to find the

page, or came to a conclusion that the content was not infringing. This was all about individual links to infringing content, but the latest change to Google's search algorithm will focus on entire websites. The ones most likely to be affected are mentioned in Google's online transparency report. The company ranked websites by the number of takedowns received: RapidGator, 4Shared and Dilandau were the most often mentioned last year – each of them accounted for over 7 million DMCA notices.

The BPI appeared the most active takedown-sender last year, submitting over 43 million notices to Google. The British anti-piracy outfit admitted that it would like to see other search engines, including Bing and Yahoo, follow the suit. The BPI is also pressing for Google to delist

entirely websites that have been ruled against the law by the courts. They include portals blocked by British Internet service providers: The Pirate Bay, Kickass Torrents, H33T, Fenopy, and another 21 websites. However, Google may push back against this pressure from the British outfit, claiming that it would be inappropriate to remove entire websites instead of certain links. Finally, the BPI demands Google to be faster at removing "pirate applications" from Android's Google Play Store.

Q.3 An extra copy maintained by administrators or users to be used in recoveries and failures

- a) Data Warehouse b) RAID c) Backup d) Shadow Files

Q.4 Technology for updating a web page without refreshing the page itself

- a) Ajax b) JavaScript c) JQuery d) JSON

Google Offers Physical USB Security Key

- Nitish Vyas

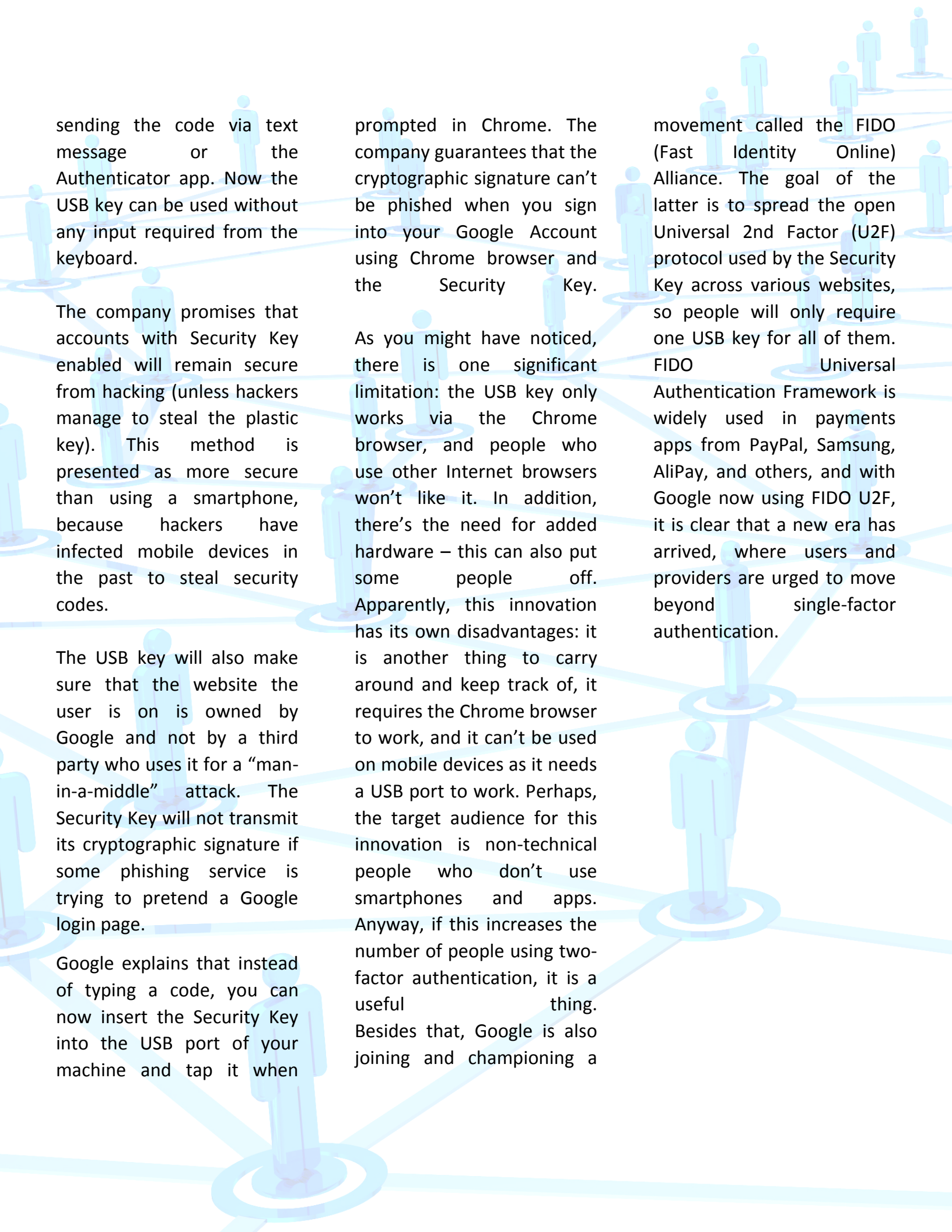
The tech giant has finally announced a physical USB Security Key for two-factor authentication. The key is expected to ensure that users keep their accounts safe from intruders, but it has its own limitations. Users

can buy a compatible USB from a third-party supplier and add the Security Key functionality. After doing so, they can start using it when logging in to Google's services, including Gmail and Google Drive. The key will contain the code required for two-factor authentication, if the latter has been switched on. Two-factor authentication is a popular method of

security protection. It required both a password and an additional data able to verify the identity of the person logging in.



Before, Google provided users with the second piece of authentication data by



sending the code via text message or the Authenticator app. Now the USB key can be used without any input required from the keyboard.

The company promises that accounts with Security Key enabled will remain secure from hacking (unless hackers manage to steal the plastic key). This method is presented as more secure than using a smartphone, because hackers have infected mobile devices in the past to steal security codes.

The USB key will also make sure that the website the user is on is owned by Google and not by a third party who uses it for a “man-in-a-middle” attack. The Security Key will not transmit its cryptographic signature if some phishing service is trying to pretend a Google login page.

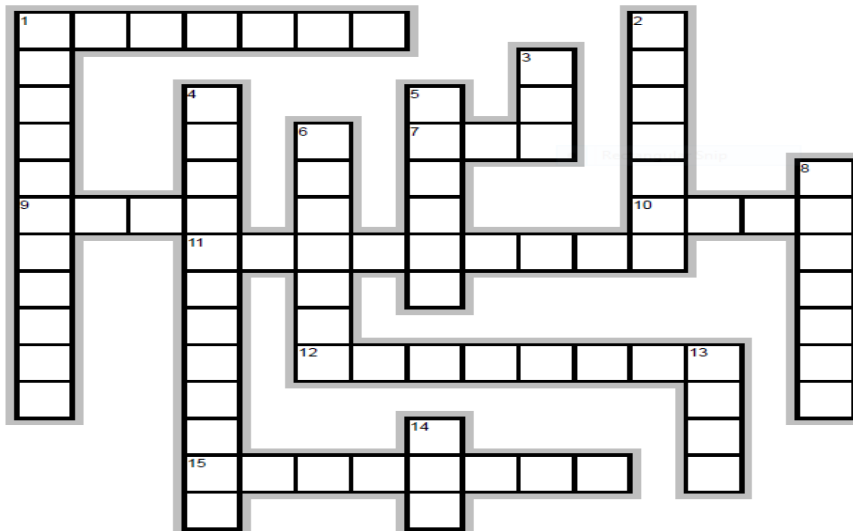
Google explains that instead of typing a code, you can now insert the Security Key into the USB port of your machine and tap it when

prompted in Chrome. The company guarantees that the cryptographic signature can't be phished when you sign into your Google Account using Chrome browser and the Security Key.

As you might have noticed, there is one significant limitation: the USB key only works via the Chrome browser, and people who use other Internet browsers won't like it. In addition, there's the need for added hardware – this can also put some people off. Apparently, this innovation has its own disadvantages: it is another thing to carry around and keep track of, it requires the Chrome browser to work, and it can't be used on mobile devices as it needs a USB port to work. Perhaps, the target audience for this innovation is non-technical people who don't use smartphones and apps. Anyway, if this increases the number of people using two-factor authentication, it is a useful thing. Besides that, Google is also joining and championing a

movement called the FIDO (Fast Identity Online) Alliance. The goal of the latter is to spread the open Universal 2nd Factor (U2F) protocol used by the Security Key across various websites, so people will only require one USB key for all of them. FIDO Universal Authentication Framework is widely used in payments apps from PayPal, Samsung, AliPay, and others, and with Google now using FIDO U2F, it is clear that a new era has arrived, where users and providers are urged to move beyond single-factor authentication.

Cyber Tech Cross Word Puzzle- Contributed By: Yogendra Singh



Across

1. Data leakage can be exploited using this kind of attack.
7. This protocol is used by skype in data transmission.
9. Metasploit framework is developed in this language.
10. Name of a Center recently proposed by Central government of India for handling Cyber Related Cases.
11. It is a process that can be applied to both digital images and audio files
12. A script that runs just after booting process is complete in Windows
15. If you know the difference between the Internet and an intranet then you can easily guess the third one.

Down

1. Hacking is legal in this profession commonly called as
2. It is the act of posting or sending offensive messages over the Internet
3. A protocol that works on two ports in a combine manner, one for data & other for control connection
4. Software Cracks are generated using this famous tool.
5. A hardware device used to bypass BIOS protection.
6. A challenge-response test that determines whether a user is human or an automated bot
8. This Microsoft-based technology was built to link desktop applications to the World Wide Web
13. It is a data type used to store large amounts of character data
14. passwords once used in login to a website are stored in this memory space

Departmental News

National Conference on Cyber Security visit- Ground Zero Summit 2014

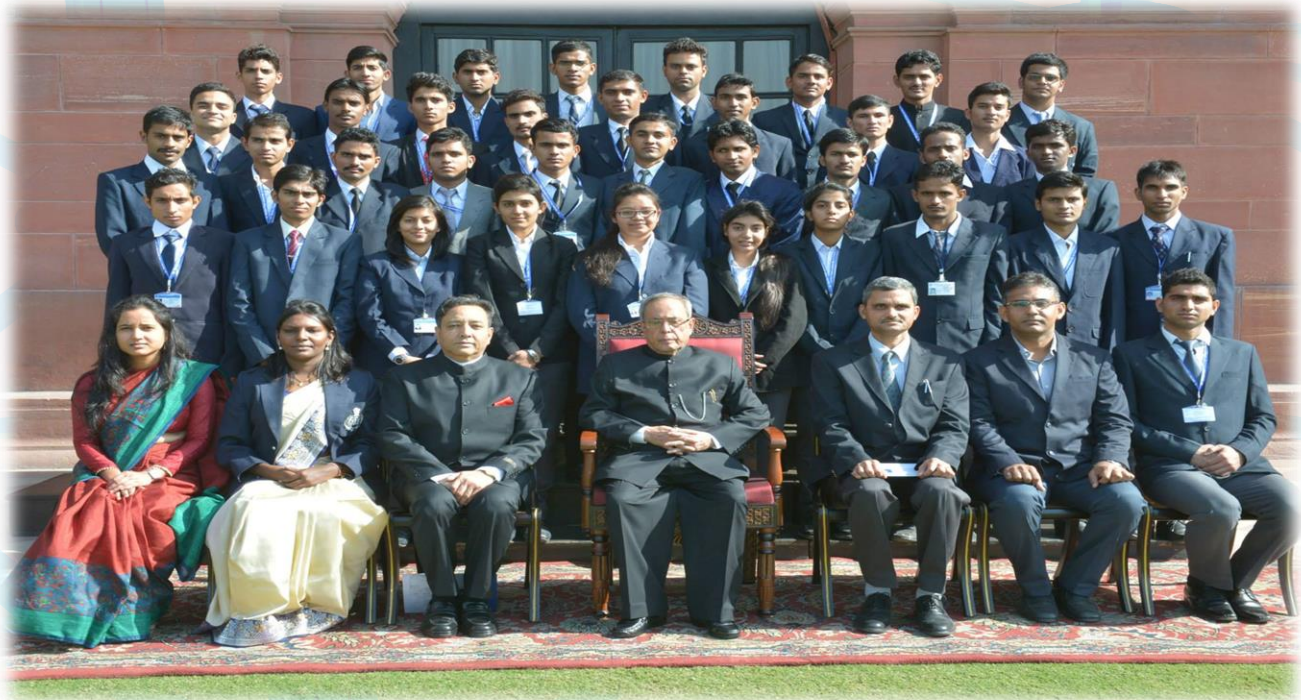
SPUP students attended Ground Zero Summit 2014 which was held in Delhi on 13-14 Nov. 2014. This summit is the largest collaboration platform in Asia for cyber security experts and researchers to address emerging cyber security challenges and demonstrate cutting edge technologies.

Ground Zero Summit is being organized by the Indian InfoSec consortium which is an independent not-for-profit organization formed by leading cyber experts.



Students of SPUP addressed by President of India

A group of students from Sardar Patel University of Police, Security and Criminal Justice, Jodhpur, Rajasthan meet the President of India, Shri Pranab Mukherjee at Rashtrapati Bhavan.



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

Editorial Board:

Pragya Johari, Vikas Yadav

Nitish Vyas, Hetram Yadav



Brought out by the Department of Computer Science & Cyber Security

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



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 issue.