INFORMATION TECHNOLOGY GENERATION CLOUD COMPUTING WIRELESS NETWORK ARCHITECTURE

# the BIT

April - August 2015

## the Bullettin of Information Technology

FACULTY CORNER

**SUSTAINABLE DEVELOPMENT TECHNOLOGY LED INNOVATION AND DEVELOPMENT**

NEW @ IT

**TRENDING NEW TECHNOLOGIES**

**INTERNET OF THINGS**


Department of Information Technology
Rajagiri School of Engineering & Technology
Rajagiri Valley, Kakkand, Kochi
http://www.rajagiritech.ac.in

RSET
RAJAGIRI SCHOOL OF ENGINEERING & TECHNOLOGY

# Sustainable Development –Technology led Innovation and research

We can see the emergence of an array of increasingly vibrant movements to harness science and technology in the quest for a transition towards sustainability. The key tenet of sustainability is adopting an integrated, holistic view of economic, social, and environmental systems (tri -pillar model). There is a great reliance on technology to solve environmental problems around the world today. To meet this sustainability challenges more focus is to be given to the dynamic interaction between nature and society with equal importance to how social change shapes environment and how environmental change shapes society.

How science and technology could contribute more effectively to sustainable development? The involvement of researchers, practitioners, academic institutions and development organizations from all around the world was seriously discussed in various forum. Large number of international science based assessments for environmental protection are incorporating sustainability concerns. Also variety of sustainable technology based efforts are taking place at local, regional, and national levels all around the world. Again academic institutions are offering courses and doing research to educate their stakeholders and to promote sustainable development. The results of these efforts are relatively slow and non-familiar beyond their location. The innovations produced as a result of these developing technologies should be brought to market and among the masses.

Technology should become a catalyst at the initial stage of strategic planning, merging with market insights to produce truly innovative products and ideas towards sustainable development. Sustainable technology is not an autonomous field or discipline, but rather a vibrant arena that is bringing together scholarship and practice, global and local perspectives, and disciplines across the natural and social sciences, engineering, and medicine.

Develop human resource for working together towards a common vision can ensure creative and productive development-development that meets the needs of the present without compromising the ability of future generations to meet their own needs.

KUTTYAMMA A J
PROFESSSOR & HOD, DIT

# the BIT

the Bullettin of Information Technology

ON CREATIVE DESK

Editors

PROF. KUTTYAMMA A.J.
(HOD- Department of Information Technology)

ABEY ABRAHAM
Assistant Professor

Student Editors

SNEHA P BIJOY -S7 IT

Designed by

KRISHNADAS NADUVATH
Programmer

Photo Courtsey

Google Images


## Contents

# Internet of Things -Applications,challenges &Barriers

Divya James-Assistant professor,DIT

Imagine a world in which every device in the home, workplace and car are connected. A world where the lights automatically turn on when the car approaches the driveway, the coffee starts brewing when the morning alarm goes off and the front door automatically unlocks when approached by a member of the household, but stays locked when a stranger arrives on the front step. That is the type of world the Internet of Things can create.

The Internet of Things (IoT) is a computing concept that describes a future where everyday physical objects will be connected to the Internet and will be able to identify themselves to other devices. The term is closely identified with RFID as the method of communication, although it could also include other sensor technologies, other wireless technologies, QR codes, etc.

In the context of “Internet of Things” a “thing” could be defined as a real/physical or digital/virtual entity that exists and move in space and time and is capable of being identified. Things are commonly identified either by assigned identification numbers, names and/or location addresses.

The Internet of Things allows people and things to be connected Anytime, Anyplace, with Anything and Anyone, ideally using Any path/network and Any service. The Internet of Things implies a symbiotic interaction among the real/physical, the digital/virtual worlds: physical entities have digital counterparts and virtual representation; things become context aware and they can sense, communicate, interact, exchange, data, information and knowledge.

**Applications of IoT**

The potentialities offered by the IoT make it possible to develop numerous applications based on it, of which only a few applications are currently deployed. In future, there will be intelligent applications for smarter homes and offices, smarter transportation systems, smarter hospitals, smarter enterprises and factories.

In the following sections, some of the important example applications of IoT are briefly discussed.

**Telecommunications Industry**

IoT will create the possibility of merging of diverse telecommunication technologies and create new services. An illustrative example is the use of GSM, NFC (Near Field Communication), low power Bluetooth, WLAN, multi-hop networks, GPS and sensor networks together with SIM-card technology. In these types of applications the reader (i.e., tag) is a part of the mobile phone, and different applications share the SIM-card.NFC enables communications among objects in a simple and secure way just by having them close to each other. The mobile phone can therefore be used as a NFC reader and transmit the read data to a central server. When used in a mobile phone, the SIM-card plays an important role as storage for the NFC data and authentication credentials (like ticket numbers, credit card accounts, ID information etc). Things can join networks and facilitate peer-to-peer communication for specialized purposes or toincrease robustness of communications channels and networks. Things can form adhoc peer-to-peer networks in disaster situations to keep the flow of vital information going in case of telecommunication infrastructure failures.

**Medical and Healthcare Industry**

IoT will have many applications in the healthcare sector, with the possibility of using the cell phone with RFID-sensor capabilities as a platform for monitoring of medical parameters and drug delivery. The advantage gained is in prevention and easy monitoring of diseases, ad hoc diagnosis and providing prompt medical attention in cases of accidents. Implantable and addressable wireless devices can be used to store health records that can save a patient’s life in emergency situations, especially for people with diabetes, cancer, coronary heart disease, stroke, chronic obstructive pulmonary disease, cognitive impairments, seizure disorders and Alzheimer’s disease. Edible, biodegradable chips can be introduced into human body for guided actions. Paraplegic persons can have muscular stimuli delivered via an implanted smart thingcontrolled electrical simulation system in order to restore movement functions.

**Independent Living**

IoT applications and services will have an important impact on independent living by providing support for an

aging population by detecting the activities of daily living using wearable and ambient sensors, monitoring social interactions using wearable and ambient sensors, monitoring chronic disease using wearable vital signs sensors, and in body sensors. With emergence of pattern detection and machine learning algorithms, the things in a patient's environment would be able to watch out and care for the patient. Things can learn regular routines and raise alerts or send out notifications in anomaly situations.

**Media, Entertainment Industry**

Deployment of IoT technologies will enable ad hoc news gathering based on locations of the users. The news gathering could happen by querying IoT, to see which multimedia-capable devices are present at a certain location, and sending them a (financial) offer to collect multimedia footage about a certain event. Near field communication tags can be attached to posters for providing more information by connecting the reader to an URI address that contains detailed information related to the poster

**Environment Monitoring**

Utilization of wireless identifiable devices and other IoT technologies in green applications and environmental conservation are one of the most promising market segments in the future. There will be an increased usage of wireless identifiable devices in environmentally friendly programs worldwide.

**Challenges and Barriers to IoT**

Several barriers, however, have the potential to slow the development of IoT. The three largest are the deployment of IPv6, power for sensors, and agreement on standards.

**Deployment of IPv6**

The world ran out of IPv4 addresses in February 2010. While no reali mpact has been seen by the general public, this situation has the potential to slow IoT's progress since the potentially billions of new sensors will require unique IP addresses. In addition, IPv6 makes the management of networks easier due to auto configuration capabilities and offers improved security features.

**Sensor energy**

For IoT to reach its full potential, sensors will need to be self-sustaining.Imagine changing batteries in billions of devices deployed across the planet and even into space. Obviously, this isn't possible. What's needed is a way for sensors to generate electricity from environmental elements such as vibrations, light, and airflow.18 In a significant breakthrough, scientists announced a commercially viable nanogenerator—a flexible chip that uses body movements such as the pinch of a finger to generate electricity—at the 241st National Meeting & Exposition of the American Chemical Society in March 2011.

**Standards**

While much progress has been made in the area of standards, more is needed,especially in the areas of security, privacy, architecture, and communications. IEEE is just one of the organizations working to solve these challenges by ensuring that IPv6 packets can be routed across different network types.

**Next Steps**

IoT is at a stage where disparate networks and a multitude of sensors must come together and interoperate under a common set of standards. This effort will require businesses, governments, standards organizations, and academia to work together toward a common goal.

Next, for IoT to gain acceptance among the general populace, service providers and others must deliver applications that bring tangible value to peoples' lives. IoT must not represent the advancement of technology for technology's sake; the industry needs to demonstrate value in human terms.

In conclusion, IoT represents the next evolution of the Internet. Given that humans advance and evolve by turning data into information, knowledge, and wisdom, IoT has the potential to change the world as we know it today—for the better. How quickly we get there is up to us.

# Tabnabbing: A New Type of Phishing Attack

MANJU V.J NE,S2-MTECH

Everyone wanted to be hacker these days. The availability of the tools and techniques on the internet motivating everyone to hack. With this, situation has totally gone worst. We're much aware of the social and professional networks like Twitter and LinkedIn being hacked in the past. In this article I intend to talk about a new type of phishing attack called Tabnabbing.

Tab Nabbing technique is a type of phishing attack which persuades the users to submit their login details like username and password of the websites like Facebook by impersonating them.

The Tab Nabbing script is hosted on the website or blog which exploits when the visitor reads an article or play some media or a game.

One can't just browse a single tab on his browser these days. This behavior of the common internet browser user is the key issue in inventing this attack.

When the victim visit the website or blog you had the script hosted on, along with the tabs with Facebook logged in, this technique can be exploited. When the victim goes to Facebook tab from your website and comes back, your website shows a phishing page asking him to log-in with Facebook. If he enter login details in that phishing page, he'll be hacked.

Facebook or any other account can be hacked using the Tab Nabbing technique. Gaming on Facebook has become a fashion for the users. They don't really know what they are getting into when they click a couple of 'Okay's before they start playing. Tabnabbing operates in reverse of most phishing attacks in that it doesn't ask users to click on a obfuscated link but instead loads a fake page in one of the open tabs in your browser.

This is how tabnabbing works:

- You have a bunch of open tabs in your web browser, an e-mail page, Facebook, your bank account and maybe a bunch of news sites.
- While you're reading your favorite Mashable.com content, the attack is able to hone in on tabs that haven't been used or aren't in focus and replace the favicon (the icon in your tab bar) and the title of the tab.
- When you click on that tab, a fake page is loaded in its place, maybe it is loaded to look like a standard login page.
- Because you already had this tab open legitimately before, you don't bother paying any attention to the URL in the address bar and you enter in your login information.
- You've just sent your info to a nefarious third party.

This is what you can do to keep yourself safe from these types of attacks:

- Keep your web browser up-to-date. Also make sure that plugins and extensions are up-to-date and from trusted sources.
- If you're a Windows user, make sure you have anti-virus or anti-malware software on your computer
- Pay attention to the address in your browser's toolbar, especially when it comes to login pages. It's easy to get into muscle-memory mode and just assume that a tab is unchanged, but for important user accounts, keep an eye on that location bar.

# SOCIAL ENGINEERING ATTACKS

SRUTHY SANTHOSH NE, S4 - M.TECH

1. QUID PRO QUO

Quid pro quo attacks promise a benefit in exchange for information. This benefit usually assumes the form of a service, whereas baiting frequently takes the form of a good.

One of the most common types of quid pro quo attacks involve fraudsters who impersonate IT service people and who Spam call as many direct numbers that belong to a company as they can find. These attackers offer IT assistance to each and every one of their victims. The fraudsters will promise a quick fix in exchange for the employee disabling their AV program and for installing malware on their computers that assumes the guise of software updates.

It is important to note, however, that attackers can use much less sophisticated quid pro quo offers than IT fixes. As real world examples have shown, office workers are more than willing to give away their passwords for a cheap pen or even a bar of chocolate.

Quid pro quo is a Latin phrase that literally means "something for something." The phrase usually indicates an exchange of

goods or services of roughly equivalent value.


From a legal perspective, quid pro quo indicates that a good or service has been traded for something of equal value. In particular, quid pro quo is used explicitly to indicate that there has been “consideration” in a contract, meaning that there are goods or services being delivered and that acceptable payment is made for these goods or services. Without consideration, or quid pro quo, for example, a contract may be determined to be non binding and invalid.

In the political world, for example, quid pro quo sometimes refers to giving support, financial or otherwise, to a political candidate in exchange for the expectation of direct support for an activity of the political benefactor. Quid pro quo may appear as bribery in these cases and such support must always be tested for conflicts of interest.

Quid pro quo is one of the most common Latin legal terms used. In any transaction, legal, political or otherwise, it is helpful to know the quid pro quo, that is, the balance of the value of the service or good and the financial compensation being offered.

**2.TAILGATING**

Another social engineering attack type is known as tailgating or “piggybacking.” These types of attacks involve someone who lacks the proper authentication following an employee into a restricted area.


In a common type of tailgating attack, a person impersonates a delivery driver and waits outside a building. When an employee gains security’s approval and opens their door, the attacker asks that the employee hold the door, thereby gaining access off of someone who is authorized to enter the company.

Tailgating does not work in all corporate settings, such as in larger companies where all persons entering a building are required to swipe a card. However, in mid-size enterprises, attackers can strike up conversations with employees and use this show of familiarity to successfully get past the front desk. To describe the act of an unauthorized person who follows someone to a restricted area without the consent of the authorized person, the term tailgating is also used. “Tailgating” implies without consent (similar to a car tailgating another vehicle on the freeway), while “piggybacking” usually implies consent of the authorized person.

Piggybacking can be regarded as one of the simpler forms of social engineering.

Many locations are too secure to allow simple piggybacking. These may include those with intense human surveillance or three-dimensional computer vision detection systems, such as those at airports, apartments with doormen, or turnstiles.

Others, with weaker controls, are more likely to allow such a breach. These may include unmanned entries with the use of a card or entry code, or locations where an attendant can be easily distracted by high traffic or other duties.

High-security facilities typically use secure revolving doors or “mantraps” to prevent tailgating. Revolving doors may have a smaller segment space between the door leaves, and can be fitted with electronic sensors using infrared beams and computer vision systems which cause the door’s powered rotation to reverse if more than one person is detected in a segment space. Alternatively, a Gatekeeper system can be used which applies photonics technology to measure the volume occupied by one person; two persons occupy a larger space and as such are not allowed to enter

# Tools Used For Hacking The System

MATHEWS ABRAHAM NE,S4-MTECH

Hackers use a variety of tools to attack a system. Each of the tools have distinct capabilities.

**Port scanners**
**Rootkits**
**Sniffers**

**Port Scanners**

Port scanners are probably the most commonly used scanning tools on the Internet. These tools scan large IP spaces and report on the systems they encounter, the ports available, and other information, such as OS types. The most popular port scanner is Network Mapper (Nmap).

Nmap ("Network Mapper") is an open source utility for network exploration or security auditing. It was designed to rapidly scan large networks, although it works fine against single hosts. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (ports) they are offering, what operating system (and OS version) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. Nmap runs on most types of computers, and both console and graphical versions are available. Nmap is free software, available with full source code under the terms of the GNU GPL.

Nmap is an excellent security tool because it allows you to determine which services are being offered by a system. Because Nmap is optimized to scan large IP ranges, it can be run against all IP addresses used by an organization, or all cable modem IP addresses provided by an organization. After using Nmap to find machines and identify their services, you can run the Nessus vulnerability scanner against the vulnerable machines. Tools Nmap supports an impressive array of scan types that permit everything from TCP SYN (half open) to Null scan sweeps. Additional options include OS fingerprinting, parallel scan, and decoy scanning, to name a few.

**Rootkits**

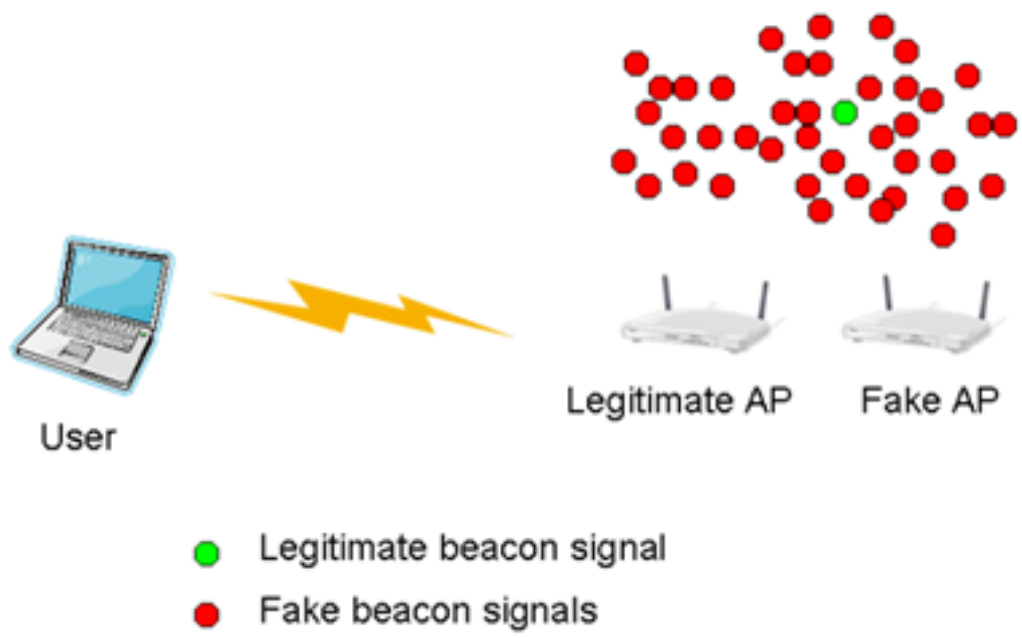
Rootkits The term rootkit describes a set of scripts and executables packaged together that allow intruders to hide any evidence that they gained root access to a system. Some of the tasks performed by a rootkit are as follows:

Modify system log files to remove evidence of an intruder's activities.

Modify system tools to make detection of an intruder's modifications more difficult.

Create hidden back-door access points in the system.

Use the system as a launch point for attacks against other networked systems




**Sniffers**

Sniffers Network sniffing, or just "sniffing," is using a computer to read all network traffic, of which some may not be destined for that system. To perform sniffing, a network interface must be put into promiscuous mode so that it forwards, to the application layer, all network traffic, not just network traffic destined for it. The Solaris OE includes a tool called snoop that can capture and display all network traffic seen by a network interface on the system. While being relatively primitive, this tool can quite effectively gather clear-text user IDs and passwords passing over a network. Many popular protocols in use today such as Telnet, FTP, IMAP, and POP-3 do not encrypt their user authentication and identification information.

Once a system is accessed, an intruder typically installs a network sniffer on the system to gain additional user ID and password information, to gather information about how the network is constructed, and to learn what it is used for.

**Bluetooth Attack Tools**

The number of tools available to attack Bluetooth devices is also growing with the growing popularity of Bluetooth devices. For DoS attacks, the BlueSmack tool can be used to launch the ping of death attack on Bluetooth devices. It works by requesting an echo from a Bluetooth device. When thousand of these echoes are requested, the device cannot service anything but the echoes and causes a DoS. Other DoS tools include BlueChop and BluePass .

BlueChop can be used to disrupt the established piconet and BluePass can be used to create Bluetooth packets to cause the buffer overflow attack. BlueSnarf is a tool that can be used for bluesnarfing. Again means obtaining unauthorized files from a Bluetooth device by keeping the connection open and requesting those file.

BlueBump is a tool that can be used to obtain the victim's key. Some PDAs will allow an attacker to request a key regeneration that can be used later to gain full access to the system. The table below summarizes the Bluetooth attack tools presented. As Bluetooth technology becomes more prevalent in user's everyday lives and as more product become available, more attack tools will emerge.

There are several DoS attacks that can be used to disrupt normal Bluetooth communication. Also there are attacks to gain full access to a victim's device. All of which can cause major problems for the user.

# Cyber Security & Deep Web

MOHAMED JASIM. M NE,S2 -M.TECH

The world have changed significantly from Stone Age to information era, even money is evolved into digital information. Have you ever anticipated about the most expensive currency today? It is the "Bitcoin" which doesn't have a physical existence, currently it has more value than the sum of top 54 currencies in the world and which can be used across the boundaries. As the relevance of information exchange is getting more crucial, the thief have sold their mask and bought a "blackhat". Blackhat hackers are computer criminals who break into secure networks to destroy, modify, or steal data.

A beginner to hacking (known as script kiddies) are familiar with Keyloggers, Wi-Fi hacking, Hview, etc, while the advanced hackers play off the ground in the deep web.

Hacking can be simply defined by:-

```
if(condition 1)
{       try a,b,c….n
}
elseif(condition 2)
{       try d,e,f…n
}
.
.
elseif(condition n)
{       try p,q,r…n
}
where n -> ∞
```

Hacking is hard as understanding the above piece of code for an individual with weak programming knowledge. An elite hacker can be considered as the one who is able to find the exact condition and the best possible combinations of "try" to break through in minimum time. In order to become an elite hacker, extensive technical skills as well as knowledge about the target is required, which is the most challenging part. Thus a best hacker is the one who finds a way to peep through the keyhole of the barrier.

Hacking is basically stealing the sensitive information which is wrapped by a bunch of nonsense materials know as encryption.

Indian Government websites are the major victims of Sql injections, Sql injection is a method of writing the SQL queries in the field of input texts, authentication details such as email address and password. Sql injection is prevented by using 'Prepared Statements' in SQL but brute force attack cannot be prevented. Brute force attack is the process of trying all possible combinations in a linear way which require extensive resources, Blackhat hackers utilizes CUDA, graphic programming which turns the High GPU Graphic processors to do the job.

Sample SQL query:-

```
select client from table_client  where client_
password='/*user input*/'
```

Web users utilize the password input field to manipulate the SQL database or alter the query and fetch information from database. In advanced SQL injection, the hacker utilizes the html post to manipulate the database.

Intruders' manipulation:-

```
select client from table_client  where client_
password = 'name' or 'a'='a';
```

The addition of the OR 'a'='a' condition causes the where clause to always evaluate to true, so the query becomes logically equivalent to the much simpler query.

## Common Vulnerable Tools & Techniques:

### Keyloggers:

Keyloggers are computer programs designed to work on the target computer's software. Keyloggers are used in IT organizations to troubleshoot technical problems with computers and business networks. This tool is utilized by script kiddies to steal the password. keyloggers records each keystrokes in keyboard and some are capable of taking screen shorts and even send it to remote system.

Anti-virus programs are capable of detecting most of the keyloggers but script kiddies are smart enough to utilize the exemption folder in anti-virus programs. So in order to make sure your boyfriend is not reading all your keystrokes, make sure the exemption folder of your anti-virus program doesn't contain any RAT (Remote administrative tools) files to prevent an early breakup.

### Wi-Fi hacking (Cracking WEP):

Password of router is traced by using various techniques such as using backtrack OS, a Linux based OS in which a series of codes are used, which track the routers responses to each wrong combinations and finally interrupt the actual value which the router use to compare.

The biggest flaw probably in a WEP key is that it supports only 40bit encryption which means that there are 16million possibilities only.

Here is what you would require to crack a WEP key:

1. Backtrack or any other Linux distro with aircrack-ng installed

2. A Wifi adapter capable of injecting packets , For this tutorial I will use Alfa AWUS036H which is a very popular card and it performs well with Backtrack

To begin, you'll need to first put your wireless adapter into monitor mode , Monitor mode is the mode whereby your card can listen to every packet in the air. Now a new interface mon0 will be created , After putting your card into monitor mode ,we need to find a network that is protected by WEP. To crack the WEP key you'll have to capture the targets data into a file, and save the captured data.

The console command used to crack the WEP key: aircrack-ng (name of the file)

### Hview:

A tool which transforms the script kiddies to some serious hacker, Hview gives a transparent view of the codes running in a process and some statements like jump is used to bypass the authentication phase. Generally used to create pirate versions of games, software, etc… hview is a Curses-based hex editor designed to work with large (600+MB) files as quickly and with as little overhead as possible.

### Deep web:

It's said that, we just have access to 1% of the internet and rest lies in the deep web where all the illegal online trades like drugs, weapons, ammunitions, contract killers, fake passports, bank accounts, etc… this is also the playground for terrorists and blackhat hackers, because they cannot be traced. In Deep web bitcoins are used for transactions and even clients use various encryption methods like MD5 to transfer their details.

The deep web or Invisible web is the part of internet that is not indexed by standard search engines. To discover contents on the web, search engines use web crawlers. This technique is ideal for discovering contents on the surface web but ineffective at finding deep web content. A darknet is an overlay network that can only be accessed with specific software, configurations often using non-standard communication protocols and ports. Two typical darknet types are friend-to-friend networks (usually used for file transfer & p2p connection) and anonymous peer-to-peer network such as Tor.

Darknets in generally may be used for various reasons, such as:-

- To better protect privacy from targeted and mass surveillance
- Protecting dissidents from political reprisal
- Whistleblowing and news leaks

- Computer crime
- Buy restricted goods on darknet markets
- File sharing

All darknets require specific software installed or network configurations made to access them. Different darknet services are:-

- Tor (The onion router): is an anonymity network. It is the most popular instance of darknet.
- I2P (invisible internet Project): is another overlay network that features a darknet whose sites are called “Eepsites”.
- Freenet: is a popular darkent, it can run as a “opennet”(peer nodes are discovered automatically).
- RetroShare: It can be run as darknet by default to perform anonymous file transfers if DHT and discovery features are disabled.
- GNUnet: it is a software used to publish distributed forums over the anonymous networks of I2P, Tor and Freenet.
- OneSwarm can be run as a darknet for Peer-to-Peer file sharing.
- Tribler can be run as darknet for file sharing.

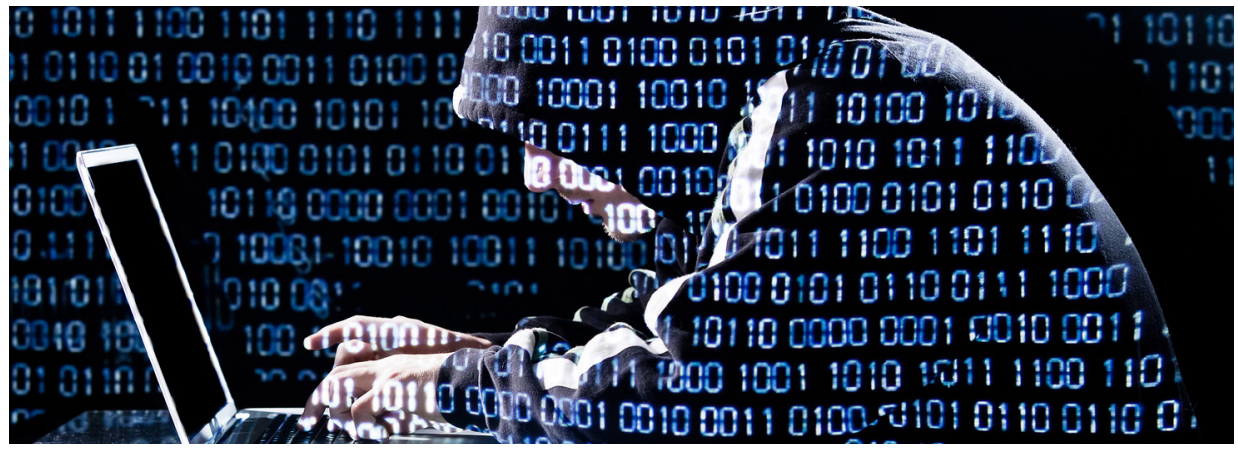
**TOR Browser:**

Onion routing was initially designed at the US Naval Research Laboratory to protect the security and privacy of network communications. Tor was originally designed to shield intelligence gathering operations from open sources and protect military communications over public networks. The network works by routing traffic through multiple nodes in an effort to help mask the identities of its users.

Onion routing is a technique for anonymous communication over a computer network. In an onion network, messages are encapsulated in layers of encryption, analogous to layers of the vegetable onion.

# HOW TO HACK A FACEBOOK ACCOUNT

TESSA AUGUSTINE S6- IT



Here is an interesting tip on how to hack a Facebook account by the method of reverting the password.This method does not involve any skill or anything just a brain would be enough to get you through this trick ! Well,you might think that it is impossible but it is actually true that you can hack any facebook account ! So before we start i would like to tell you what “Reverting” actually means...

Reverting is the process of resetting a password without the knowledge of the actual user ! So this is basically a low level of hacking but it does the job for you ! For more on reverting go here: What exactly is reverting ? How do I hack my friend’s Facebook ?

Make sure your not logged in to your account. If you are then make sure you sign out and then follow the following methods

1.Go to this link:
http://www.facebook.com/help/contact.php?show_form=hack_login_changed / http://www.facebook.com/help/contact.php?show_form=hacked_cannot_identify
That is the form that you will be using in order to hack your user.

2.Then in “Your E-mail Address” type your E-mail address.

3.Then apply the following options as in the image below.

4.Once you have done that,You will have a question asking “Email associated with the compromised account.” – In that just type “No” and nothing else other than that !

5.In “Your contact email address.” – Type your own email for you to receive the Password Reset Link.

6.In the “Full Name of the Account.” – Type the Name of your victim if you know. If you don’t then:
a.Try finding the Name of the victim by just searching his/her e-mail on Facebook.

b.If that doesn’t work then google the E-mail address of your Victim, that might give you some details.

c.If that also doesn’t work then use the following sites to get them
http://com.lullar.com/ http://www.pipl.com/email/

So if you follow one of the above methods you should be getting the Full Name of your victim.Now lets move on to the next step

7.”Date Of Birth” – In this column you have to enter the Birthday of your Victim.If you know him personally then you should be knowing it.If not you can just social engineer him and somehow make him tell it.Once you get it you have to enter it in that.

8.”URL (web address) of your compromised profile.” – This is just the profile URL of your Victim which can be got easily(Usually of the form: http://www.facebook.com/profile.php?id=99999)

9.Now your all set ! Before you submit the form just make sure you recheck the whole form if you have done the right thing.Once you do so just click on “Submit”

10.Thats it ! You have done it ! Now you just have to wait for Facebook team to look up for your request ! Once they approve it they will send a link to reset your victim’s Password !

# IT RIDDLES

## SNEHA P BIJOY –S6 IT

Riddle : How do you crash a PC?

Answer : Switch it on.

Riddle : How does Bill Gates enter his house?

Answer : He uses “windows”.

Riddle : What creature has the best aptitude for engineering?

Answer: The spider -- It has its own website.

Riddle : What did the computer eat on the moon?

Answer: Space bars.

Riddle : What do computer experts do at weekends?

Answer: Go for a disk drive.

Riddle : What do you get if you cross a computer with a ballet dancer?

Answer: The Netcracker suite.

Riddle : What is an astronaut’s favorite key on a computer keyboard?

Answer: The space bar.

Riddle : What world does a computer come from?

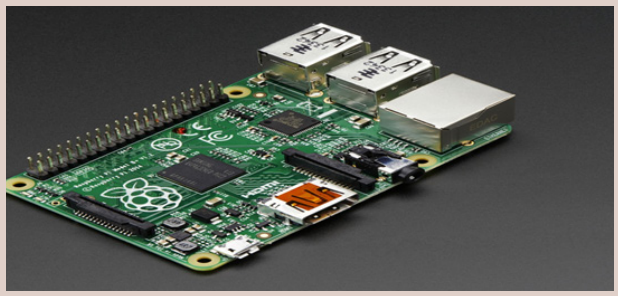
Answer: PC World.

Riddle : Why all Pascal programmers ask to live in Atlantis?

Answer: Because it is below C level.

# RASPBERRY PI

## ASHWIN VARGHESE S6- IT



The Raspberry Pi is a series of credit card-sized single-board computers developed in the UK by the Raspberry Pi Foundation with the intention of promoting the teaching of basic computer science in schools.

The original Raspberry Pi and Raspberry Pi 2 are manufactured in several board configurations through licensed manufacturing agreements with Newark element14 (Premier Farnell), RS Components and Egoman. These companies sell the Raspberry Pi online. Egoman produces a version for distribution solely in China and Taiwan, which can be distinguished from other Pis by their red colouring and lack of FCC/CE marks. The hardware is the same across all manufacturers. Raspberry Pi is based on the Broadcom BCM2835 system on a chip (SoC), which includes an ARM1176JZF-S 700 MHz processor, VideoCore IV GPU, and was originally shipped with 256 megabytes of RAM, later upgraded (models B and B+) to 512 MB. The system has Secure Digital (SD) (models A and B) or MicroSD (models A+ and B+) sockets for boot media and persistent storage.
In 2014, the Raspberry Pi Foundation launched the Compute Module, which packages a BCM2835 with 512 MB RAM and an eMMC flash chip into a module for use as a part of embedded systems.

The Foundation provides Debian and Arch Linux ARM distributions for download. Tools are available for Python as the main programming language, with support for BBC BASIC (via the RISC OS image or the Brandy Basic clone for Linux), C, C++, Java, Perl and Ruby.

As of 18 February 2015, over five million Raspberry Pis have been sold. While already the fastest selling British personal computer, it has also shipped the second largest number of units behind the Amstrad PCW, the “Personal Computer Word-processor”, which sold eight million.

In early February 2015, the next-generation Raspberry Pi, Raspberry Pi 2, was officially announced. The new computer board will initially be available only in one configuration (model B) and features a Broadcom BCM2836 SoC, with a quad-core ARM Cortex-A7 CPU and a VideoCore IV dual-core GPU; 1 GB of RAM with remaining specifications being similar to those of the previous generation model B+. Crucially, the Raspberry Pi 2 will retain the same US$35 price point of the model B, with the US$25 model A remaining on sale.

Technology writer Glyn Moody described the project in May 2011 as a “potential BBC Micro 2.0”, not by replacing PC compatible machines but by supplementing them. In March 2012 Stephen Pritchard echoed the BBC Micro successor sentiment in ITPRO. Alex Hope, co-author of the Next Gen report, is hopeful that the computer will engage children with the excitement of programming.

Use in education:

As of January 2012, enquiries about the board in the United Kingdom have been received from schools in both the state and private sectors, with around five times as much interest from the latter. It is hoped that businesses will sponsor purchases for less advantaged schools. The CEO of Premier Farnell said that the government of a country in the Middle East has expressed interest in providing a board to every schoolgirl, in order to enhance her employment prospects.

In 2014, the Raspberry Pi Foundation hired a number of its community members including ex-teachers and software developers to launch a set of free learning resources for its website. The resources are freely licensed under Creative Commons, and contributions and collaborations are encouraged on social coding platform GitHub.

The Foundation also started a teacher training course called Picademy with the aim of helping teachers prepare for teaching the new computing curriculum using the Raspberry Pi in the classroom. The continued professional development course is provided free for teachers and is run by the Foundation’s education team.

# CYBERNETICS

IRENE MARIA MATHEW S6 IT

Cybernetics is a transdisciplinary approach for exploring regulatory systems, their structures, constraints, and possibilities. Cybernetics is relevant to the study of systems, such as mechanical, physical, biological, cognitive, and social systems. Cybernetics is applicable when a system being analyzed incorporates a closed signaling loop; that is, where action by the system generates some change in its environment and that change is reflected in that system in some manner (feedback) that triggers a system change, originally referred to as a "circular causal" relationship. Some say this is necessary to a cybernetic perspective. System dynamics, a related field, originated with applications of electrical engineering control theory to other kinds of simulation models (especially business systems) by Jay Forrester at MIT in the 1950s.

Concepts studied by cyberneticists include, but are not limited to: learning, cognition, adaptation, social control, emergence, communication, efficiency, efficacy, and connectivity. These concepts are studied by other subjects such as engineering and biology, but in cybernetics these are abstracted from the context of the individual organism or device.

Norbert Wiener defined cybernetics in 1948 as "the scientific study of control and communication in the animal and the machine." The word cybernetics comes from Greekκυβερνητική (kybernetike), meaning "governance", i.e., all that are pertinent to κυβερνάω (kybernao), the latter meaning "to steer, navigate or govern", hence κυβέρνησις (kybernesis), meaning "government", is the government while κυβερνήτης (kybernetes) is the governor or the captain. Contemporary cybernetics began as an interdisciplinary study connecting the fields of control systems, electrical network theory, mechanical engineering, logic modelling, evolutionary biology, neuroscience, anthropology, and psychology in the 1940s, often attributed to the Macy Conferences. During the second half of the 20th century cybernetics evolved in ways that distinguish first-order cybernetics (about observed systems) from second-order cybernetics (about observing systems). More recently there is talk about a third-order cybernetics (doing in ways that embraces first and second-order).

Fields of study which have influenced or been influenced by cybernetics include game theory, system theory (a mathematical counterpart to cybernetics), perceptual control theory, sociology, psychology (especially neuropsychology, behavioural psychology, cognitive psychology), philosophy, architecture, and organizational theory.

Cybernetics in engineering is used to analyze cascading failures and System Accidents, in which the small errors and imperfections in a system can generate disasters. Other topics studied include:Adaptive systems, Engineering cybernetics, Ergonomics, Biomedical engineering and Systems engineering.

The term adaptation is used in biology in relation to how living beings adapt to their environments, but with two different meanings. First, the continuous adaptation of an organism to its environment, so as to maintain itself in a viable state, through sensory feedback mechanisms. Second, the development (through evolutionary steps) of an adaptation (an anatomic structure, physiological process or behaviour characteristic) that increases the probability of an organism reproducing itself (although sometimes not directly).

Generally speaking, an adaptive system is a set of interacting or interdependent entities, real or abstract, forming an integrated whole that together are able to respond to environmental changes or changes in the interacting parts. Feedback loops represent a key feature of adaptive systems, allowing the response to changes; examples of adaptive systems include: natural ecosystems, individual organisms, human communities, human organizations, and human families.

Some artificial systems can be adaptive as well; for instance, robots employ control systems that utilize feedback loops to sense new conditions in their environment and adapt accordingly.

Engineering cybernetics or technical cybernetics, established by H.S. Tsien, is a field of cybernetics, which deals with the question of control engineering of mechatronic systems as well as chemical or biological systems. It is used to control and predict the behaviour of such a system; see control theory.

An example of engineering cybernetics is a device designed in the mid-1960s by General Electric Company. Referred to as a CAM (cybernetic anthropomorphous machine), this machine was designed for use by the US Army ground troops. Operated by one man in a "cockpit" at the front end, the machine's "legs" steps were duplicates of the leg movements of the harnessed operator.

Biomedical engineering (BME) is the application of engineering principles and design concepts to medicine and biology for healthcare purposes (e.g. diagnostic or therapeutic). This field seeks to close the gap between engineering and medicine: It combines the design and problem solving skills of engineering with medical and biological sciences to advance health care treatment, including diagnosis, monitoring, and therapy. Biomedical engineering has only recently emerged as its own study, compared to many other engineering fields. Such an evolution is common as a new field transitions from being an interdisciplinary specialization among already-established fields, to being considered a field in itself. Much of the work in biomedical engineering consists of research and

development, spanning a broad array of subfields . Prominent biomedical engineering applications include the development of biocompatible prostheses, various diagnostic and therapeutic medical devices ranging from clinical equipment to micro-implants, common imaging equipment such as MRIs and EEGs, regenerative tissue growth, pharmaceutical drugs and therapeutic biological.

Systems engineering is an interdisciplinary field of engineering that focuses on how to design and manage complex engineering systems over their life cycles. Issues such as requirements engineering, reliability, logistics, coordination of different teams, testing and evaluation, maintainability and many other disciplines necessary for successful system development, design, implementation, and ultimate decommission become more difficult when dealing with large or complex projects. Systems engineering deals with work-processes, optimization methods, and risk management tools in such projects. It overlaps technical and human-centered disciplines such as control engineering, industrial engineering, software engineering, organizational studies, and project management. Systems engineering ensures that all likely aspects of a project or system are considered, and integrated into a whole.

The systems engineering process is a discovery process that is quite unlike a manufacturing process. A manufacturing process is focused on repetitive activities that achieve high quality outputs with minimum cost and time. The systems engineering process must begin by discovering the real problems that need to be resolved, and identify the most probable or highest impact failures that can occur - systems engineering involves finding elegant solutions to these problems.

# WIFIPHISHER

AISHWARYA V S4 IT

Phishing is the attempt to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money), often for malicious reasons, by masquerading as a trustworthy entity in an electronic communication.


A new Wi-Fi attack tool has been made available on GitHub that automates phishing attacks over WPA networks, putting credentials and other supposedly secret data at risk. The tool, called wifiphisher, jams Wi-Fi access points with deauthentication packets and then mimics the target access point before presenting the wireless device with a phony WPA log-in page.

It is a social engineering attack that unlike other methods it does not include any brute forcing. It is an easy way for obtaining WPA credentials.

Wifiphisher runs on Kali Linux and requires two wireless network interfaces, one capable of injections.The death packets, are sent to the client from the access point, to the access point to the client, and to the broadcast address. The jamming tool then copies settings from access points in the area and presents the victim with a phony access point. Wifiphisher also sets up a NAT and DHCP server in order to forward the right ports to the clients.

Consequently, because of the jamming, clients will start connecting to the rogue access point. An attacker, or pen-tester, would then conduct a man-in the middle attack using the rogue access point in order to sniff traffic.Users, however, won't likely automatically connect to a rogue access point. Some Windows systems, if configured to do so, will warn users of a network change. At that point, a user will have to ignore warnings and manually connect to a network.

Wifiphisher employs a minimal web server that responds to HTTP & HTTPS requests. As soon as the victim requests a page from the Internet, wifiphisher will respond with a realistic fake page that asks for WPA password confirmation due to a router firmware upgrade.Using deauthentication packets is a staple ofwifi hacking a pen-testing. Most, however, repeatedly send packets to a client and never allow it to get past the authentication process.

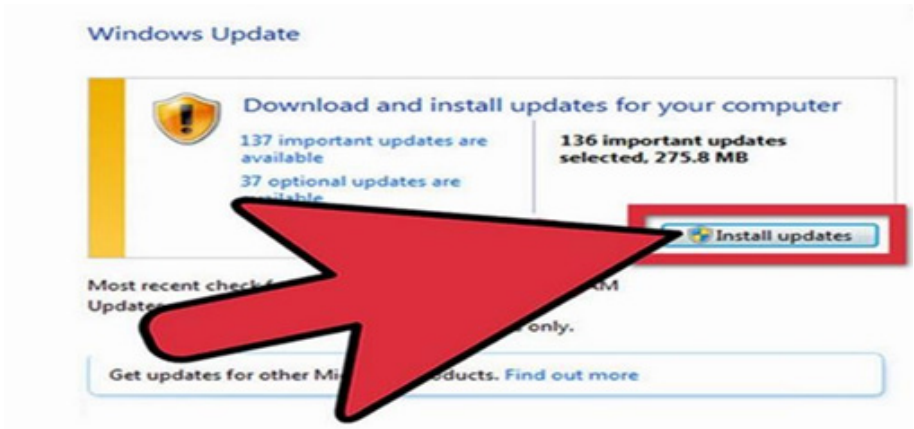
# First Aid for Hacking

MUHAMMED SADIQUE UK NE,S2-MTECH

Computer hacking can occur in a number of ways. Your computer system itself can be hacked and mined for personal information. Your blog or website can be compromised if a hacker obtains your password. Your email can be hacked if you click on a fraudulent link and you may not be able to retrieve your email and other information you've registered in your account. Use these steps to safeguard your computer and prevent computer hacking.

**1. Perform required software updates for your operating system and web browser.**

Hackers attack where they see weakness. A system that hasn't




been updated recently has flaws in it that can be taken advantage of by hackers.

• Go to the Microsoft Update website to download patches and secure the most recent version of your operating system. If you have a Mac, click on the apple in the top left of your screen and choose "Software Update."

**2. Install a firewall on your computer.** Firewalls forbid outside threats such as hackers and viruses from gaining access to your system. Personalize your firewall settings during the setup process


to reflect how much data you want to allow into your system from the Internet, and update your firewall regularly.

**3. Change your passwords often**. Use a different password for each website you regularly log into, and make sure your passwords are long and intricate so that they're harder

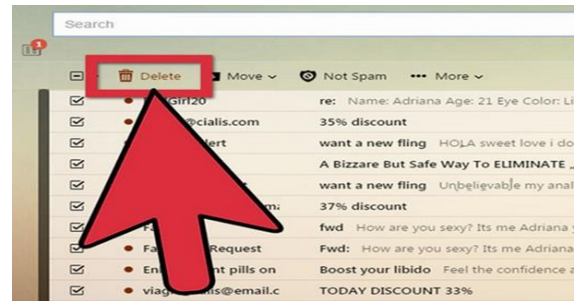
to guess. It's especially important to keep your banking and other financial accounts secure .


**4. Purchase or download anti-virus software.** Many computers come pre-installed with certain anti-virus software, but if not, or if you want more powerful software, research online to find what product suits you. Anti-virus software is crucial to keep your computer healthy. A "sick" computer, or one racked with viruses, is more susceptible to hacking. Set your preferences so your anti-virus software updates automatically.


**5. Install anti-spyware/adware programs onto your system.** This type of intrusion is not as dangerous as a virus, but adware places advertisements onto your browser and


incorporates pop-ups into your programs. This can slow down your computer, making you vulnerable to a hacker. Spyware can survey your Internet behavior and copy your passwords to use for illegitimate purposes.

**6. Delete emails from unknown sources.** Never click on an emailed link that looks questionable.




**7. Always be aware!**