CHITKARA UNIVERSITY

Department of Computer Applications
School of Computer Sciences
Chitkara University, Punjab

Wall for All

March 2016, Vol. 3, No. 1

Contents

Dawn of the Planet of Machines 1

Wearable Technology..... 3

These Mistakes can Ruin Your Careers! 5

Contact Information

Dr. Jaiteg Singh

jaiteg.singh@chitkara.edu.in

Mr. Preetinder Singh Brar

preetinder.brar@chitkara.edu.in

Mr. Vikas Rattan

vikas.rattan@chitkara.edu.in

The Dawn of the Planet of Machines

- Alisha Mehta, M.C.A. – Semester 2

Since the past centuries, man has been trying to defy the old facts and give birth to new inventions and discoveries. As we play along the lines of our boundaries and explore ourselves, we've seen major technological breakthroughs being achieved and overthrown by new and better ones. So, let us just look into the new things that are going to take over our world in no time at all.

ROBOTS

Well we have all been a great fan of these wonderful electronic devices since our childhood and have always wanted one for ourselves but with recent developments and sophisticated technological breakthroughs, this dream of ours could come true.

A new generation of robots is being introduced by companies such as Switzerland's ABB, Denmark's Universal Robots, and Boston's Rethink Robotics—robots dextrous enough to thread a needle and sensitive enough to work alongside humans.

Household robots are quite complex to program because household tasks are quite difficult to be performed by the machines. Cleaning a room needs software algorithms that are more complex than those to launch a rocket and calculate its projection. But there have been many breakthroughs of late, largely driven by A.I., enabling robots to learn tasks by themselves and teach each other what they have learnt.

ARTIFICIAL INTELLIGENCE

Artificial intelligence is the science of making intelligent machines that learn as they perform a given task. We've have all talked to Siri and Cortana but these are not as sharp as the artificially intelligent operating system Samantha in the movie Her.

In the artificial-intelligence community, there is a common saying: "A.I. is whatever hasn't been done yet". Even though computers have beaten chess masters and learnt to talk to us and drive cars, Siri and Cortana are still not as efficient.

IBM has taught its A.I. system, Watson, everything from cooking, to finance, to medicine; and Facebook, Google, and Microsoft have made achieved in developing face recognition and human-like speech systems. And IBM Watson can diagnose certain cancers better than any human doctor can.

SELF-DRIVING CARS

Once considered to be in the realm of science fiction, driverless cars made big news in 2015. Google crossed the million-mile mark with its prototypes; Tesla began releasing functionality in its cars.

Google self-driving car is a range of autonomous cars, developed by Google X as part of its project to develop technology for mainly electric cars.

Image source: http://www.bmedia4tech.com

The software installed in Google's cars is called Google Chauffeur. Because they won't crash into each other as we humans do, they are deemed to be much more safer and comfortable. Plus these cars will communicate with each other and by using the sensors in them they'll be able to track any traffic or road problems on the route they are travelling. We also won't have to worry about parking spots, because they will be able to drop us where we want to go to and pick us up when we are ready.

VIRTUAL REALITY

While sitting in India, you'll still be able to explore the Egyptian Pyramids or have a hike in the Andes or visit the castles in Europe. Yes, all of this is possible and it has been made true by Virtual Reality. In March, Facebook announced the availability of its much anticipated virtual-reality headset, Oculus. The early versions of these products are going to be expensive and not that user friendly and are going to cause dizziness .But prices will fall, capabilities will increase as is the case with all exponential technologies, and 2016 will mark the beginning of the VR revolution. Virtual reality will change the way we learn and entertain ourselves.

INTERNET OF THINGS

Just imagine this scenario: you are coming back from a long day at work and you send a simple command from your smartphone to switch on the lights, the heater, to open the gates and to turn on the coffeemaker to enjoy a good cup of coffee. Yes, this is possible by connecting the devices to one another and this is the internet of things.

Mark Zuckerberg recently announced plans to create his own artificially intelligent, voice-controlled butler to help run his life at home and at work. For this, he will need appliances that can talk to his digital butler—connected rooms, office, and car. From the showerheads playing your favourite songs while tracking the amount of water used to washing machines calculating the amount of water and detergent to be used according to the dirt in your clothes, it is all happening and coming our way.

This era indeed is the dawn of the planet of the machines as we look forward to major developments that are going to monitor our lives and make things easier for us.

Call for Articles

At Chitkara University, the endeavor has always been to hone the skills of the learners. Keeping in line with this tradition, the Department of Computer Applications, Chitkara University, Punjab had come up with an online magazine titled Wall For All. This e-magazine was proposed to provide a platform to the budding learners where they can share their knowledge and also the general information pertaining to the computing field. The e-magazine also provides an opportunity to the faculty members to share their ideas and views on topics of general interest. Wall For All is available for free download in PDF format from departmental website *ca.chitkara.edu.in*

The students as well as faculty members are encouraged to contribute articles of interest for the magazine. The articles must be original in nature, and if adapted, due credit must be extended towards that source. The students may forward the articles through their respective advisors, while the faculty members may send the same directly to the editors of Wall For All.

Wearable Technology

- Alisha Mehta, M.C.A. – Semester 2

As the world advances towards modernizing and evolving the present day technology, we are taking the next big step by developing technology that is wearable. Not only are these gadgets really handy, they are fashionable too.

The demand for these gadgets is quite high because these days they have become a fashion statement and they are associated with the tech savvy people. So, let us read a little into them.

E-textiles, also known smart textiles, or smart fabrics, are fabrics that enable digital components (including small computers), and electronics to be embedded in them.

What makes smart fabrics revolutionary is that they have the ability to do many things that traditional fabrics cannot, including communicate, transform, conduct energy and even grow.

Smart textiles can be broken into two different categories: aesthetic and performance enhancing. Aesthetic examples include fabrics that light up to fabrics that can change colour. Then there are performance enhancing smart textiles, which will have a huge impact on the athletic, extreme sports and military industries. These fabrics help to regulate body temperature, reduce wind resistance and control muscle vibration.

Jumping onto one of the bestselling wearable technology, comes the humble wrist watch which has been tweaked with to bestow us with the very efficient smart watch.

A smart watch is a computerized wristwatch with functionality that is enhanced beyond timekeeping. While early models can perform only basic tasks, such as calculations, translations, modern smart watches are effectively wearable computers as many run mobile apps, using a mobile operating system.

Some smart watches function as portable media players, playing FM radio, audio, and video files to the user via a Bluetooth headset. Some models, also called 'watch phones', feature full mobile phone capability, and can make or answer phone calls.

Image source: http://www.ugnn.com/

Most of the watches have a rechargeable battery and graphical display and many have touch screen. Peripheral devices may include thermometer, accelerometer, altimeter, barometer , compass, GPS receiver, speaker and SD card.

Software may include Map display, scheduler, calculator, and various kinds of watch face. Like other computers, a smart

watch may collect information from internal or external sensors.

It may control, or retrieve data from, other instruments or computers. It may support wireless technologies like Bluetooth, WiFi, and GPS. Smart watches are advancing, especially their user interfaces and health related applications. Motorola recently launched Moto 360 and it is loaded with so many features which have been discussed above.

Jumping onto the eyewear, here we're going to talk about smart glasses. Smart glasses or Digital Eye Glass or Personal Imaging System are a wearable computer that adds information to what the wearer sees. Typically this is achieved through an optical head-mounted display (OHMD) or computerized internet-connected glasses with transparent heads-up display (HUD) or augmented reality (AR) overlay that has the capability of reflecting projected digital images as well as allowing the user to see through it, or see better with it.

Image source: http://www.howitworksdaily.com

While early models can perform basic tasks, such as just serve as a front end display for a remote system, modern smart glasses are effectively wearable computers which can run self-contained mobile apps. These may be hands-free or they can have touch buttons.

Like other computers, smart glasses may collect information from internal or external sensors. It may control, or retrieve data from, other instruments or computers. Some smart glasses models, also feature full life logging and activity tracker capability. Google Glasses are one such device that ranks high on the popularity graph.

These smart glasses devices may also have all the features of a smartphone. Some also have activity tracker functionality features as seen in some GPS watches.

Now, a GPS watch is a device with integrated GPS receiver that is worn as a single unit strapped onto a wrist, in the manner of a watch. The watch can have other features and capabilities depending on its intended purpose. These are used for sports and fitness purposes. Many can connect to external sensors by the wireless ANT+protocol, and/or to a computer by USB to transfer data and configuration. Common sensors used are heart rate monitors and foot-pods (running cadence and speed sensor). A foot-pod can be used to supplement or replace GPS data, such as providing treadmill speed and distance for the watch to log and share. Recharging by USB is commonplace.

There are inexpensive options for fitness lovers too and these options come in the form of an activity tracker. An activity tracker is a device or application for monitoring and tracking fitness-related metrics such as distance walked or run, calorie consumption, and in some cases heartbeat and the amount of time we were in deep sleep. The term is now primarily used for dedicated electronic monitoring devices that are synced to a computer or smartphone for long-term data tracking. There are also independent smartphone apps to help us keep a check in a very proper manner.

Well, as we move forward, more things are going to get SMARTER and as we strive to make our life easier by letting these devices monitor our daily routine.

These Miskates can RUIN careers!

Preetinder Singh Brar
Associate Professor, Department of Computer Applications,
Chitkara University, Punjab

IT security, being the task assigned to the trusted few, sees few hiring, and fewer cases of firings. A pink slip being given to an IT security guy is rarely heard of. No company is willing to part with such persons, since they have complete information about the IT security architecture of the company, and also since they know just too much about the company. However, being an IT security personnel does not guarantee that you shall remain with the company for ever. One grave mistake, and you shall see your career in doldrums. In this article, a few of the mistakes that can land an IT security professional in a trouble are brought to fore.

Putting actual data through testing phase of the applications

Owing to technological advancements, and the need to handle ever-increasing volumes of data, the organisations often identify the need for implementing infrastructural upgrades.

Image source: http://www.breakthrusolution.com

The new system is usually supposed to replace the existing system. However, before putting the new system to production, stringent testing is carried out. This demands performing tests to find any trouble with database handling using the new system. In the past, numerous developers have tested this on real data. However, of late, using real data in test systems is not a preferred method, since testers often tend to be indifferent towards the test system database and are quite ruthless on that data. In fact, they have to be so, since their job is to try to fail the system rather than just checking that the new system is performing fine. Therefore, it is a better idea to generate phoney data and use it at will for testing the new system. Moreover, the test systems face an additional disadvantage. Test systems often have short passwords, and those are usually known to the whole of the testing team. In the event of any hacker trying to attack an organisation's network to gain entry to database server, then such a test system shall make the organisation a sitting duck if actual data is being used for test system.

Putting key-business functionality at risk

Each company survives because of certain pre-defined set of procedures, or protocols. If those protocols are compromised, then it may derail the core business functionality. IT security professionals agree that this is even worse than allowing the hackers gain entry to the premises of the company.

For instance, if a hacking episode has been detected by the IT security team, where the attacker has gained access to confidential data, one often finds senior management still unwilling to interrupting core business systems.

This strategy is termed as Assume Breach, wherein the organisation seems to have accepted that such unwanted activity will be found within its environment for ever, but the company should conduct business in a manner as if there's nothing unusual, since the top brass believes that the cost of damages caused by the hackers is far less than the cost of steps required to be taken to ensure that the hacker is strictly kept at bay.

Image source: http://thefinancialbrand.com

This technique seems to work some times, until the hacker causes losses worth hundreds of millions of dollars, triggering widespread outrage amongst the stakeholders, and then the responsibility of the whole episode is put solely on the shoulders of the IT security team, stating that the matter needed thorough investigation, but had IT security team indulged in dereliction of duty by not doing so.

Blocking data access by top functionaries

The IT security guys are used to blocking access to certain resources by other personnel in the organization. Most likely, they do so in good faith, as security of data is their primary concern, but in the process, they sometimes inadvertently block data access by the top brass as well.

Image source: http://www.itproportal.com

This is likely to invite trouble. The CEO, and the other key position holders, want everything, whether small or big, whether required or not, to be accessible over the network, as well as off the network. Most of those functionaries want to start using the applications by simply clicking on the icons, without the need to key-in the password, even though they may be opening some highly secured applications. It is therefore, important that the mechanism be devised so as to allow access to data for such persons in the simplest possible manner, while maintaining the required amount of security.

Ignoring the firewall alerts as false positive

All IT security personnel are aware that ignoring a critical security incident can prove lethal to their jobs. With the firewalls in place, each infiltration, whether negligible or severe, is reported and logged. The onus lies with the IT security staff to find out the intensity of the attack. In a majority of the cases, the intrusion is casually reported as false positive. Now, if the intrusion was not actually a minor one, then it may lead to losses to the tune of millions of dollars, since that intrusion, by virtue of being labelled as false positive, now becomes authorised to transfer data over the network. Take for instance, the drug formula developed by a pharmaceutical company after spending huge

money and considerable time, being transferred to the rival organisation over the wire for free due to presence of a trojan that had been reported as false positive. The rival company would be able to manufacture the same drug and would be able to bring it to market at lower cost than the actual developer, since the former had not spent any time and money on research of that drug. Imagine the losses that would be suffered by the organisation that actually developed the drug. Thus, it is prudent that all security events be scrutinized, and well-researched before reporting any false positive incident.

Reading confidential data

The network administrators, and the database administrators are amongst those employees who have full-access to the database of the organisation. These enormous powers to access the database often lead to unauthorised access of data. Unauthorised? … One may ask, then why to give rights to them if they can't access it. The answer is rather straight. The access is granted to allow managing the data, like managing the schema, backups and restore, etc. The data can be viewed only by the personnel who fulfil two necessary conditions, they should be authorised to access the data, and they should have proper clearance to view the data. Each access to database is logged with User ID, IP address, MAC ID, timestamp, and other vital parameters. These log entries also undergo stringent audit process, and if any unauthorised access is observed at any point of time, then it is a definite trouble for the person who accessed the data.

In addition to the above scenario, where organisational data is being talked of, there is another situation that pertains to accessing private data of the employees. In Indian scenario, most administrators feel that it is their right to view the data of any of the users, and most users also seem to have accepted this as an organisational protocol. However, in developed countries, there is a clear policy in most organisations in this regard, and the difference between managing and viewing the data is also clearly framed. Accessing the private data of any employee is sure to invite trouble to the administrator's job.

Image Source: http://www.usnews.com

It is in the interest of the network administrators and the database administrators, to suppress their urge to view the data that they are not permitted to view. In addition to this, the one who actually have rights to see and modify data are required to encrypt the data so that it is not accessible by anyone else. The administrators must learn that their job is to facilitate the access to appropriate persons, and should avoid any kind of moral policing by invading privacy.

CHITKARA UNIVERSITY

Corporate Office:
Saraswati Kendra
SCO 160-161, Sector 9 C,
Chandigarh 160 009
INDIA

Phones:
+91-172-2746209, 2747057

Fax:
+91-172-2746154

www.chitkara.edu.in
ca.chitkara.edu.in