CYBERSECURITY FOR THE NEW DECADES

The following articles were published by the Deccan Herald in Bangalore, India, as part of an on-going cybersecurity awareness project by Dr. S.S. Iyengar, Director and Ryder Professor of the School of Computing and Information Sciences at Florida International University and Col. Jerry Miller, Discovery Lab Research Coordinator.

VOLUME 1 - 2015-2016

Table of Contents

CYBERSECURITY FOR THE NEW DECADES

ESSENTIALS OF CYBERSECURITY

These articles are based upon wide raging discussions and information provided by a variety of researchers and cybersecurity experts around the world. We would like to acknowledge all of our colleagues and partners who are diligently working within government, public industry and academia, to combat the effects of malware and cyber-attacks.

We would specially like to acknowledge the efforts of B.S. Arun, Senior Editor at the Deccan Herald, for his assistance in publishing this articles.

We have been honoured to work with research colleagues from around the country and around the world, who are some of the best in their business and dedicated to pushing the edges of modern science and knowledge.

We would also like to thank United States Department of Defense, National Science Foundation, Oakridge National Laboratory, Jet Propulsion Laboratory, Air Force Research Laboratory, US Army Research Office and US Navy Office of Research, and a multitude of other funding agencies who have committed time and resources to support our research.

Special thanks to Ms. Ariana Taglioretti for her diligent review, creativity and support in getting this document published. We would also like to thank Dr. Mark Weiss, Dr. Shu Ching-Chen, Mr. Steve Luis, Dr. Scott Graham, and the superb faculty and staff within the School of Computing and Information Sciences at Florida International University's College of Engineering and Computing for all they do every day in providing excellence in education, research and community outrage.

1. Origins of cybersecurity

The roots of cybersecurity can be traced back long before the word "cyber" came into vogue, to what was known as information security. The actions involved in "information security," however, are as old as "information" itself. Early man wanted to protect information in order to maintain a competitive advantage in business, whether that was hunting the plains for food, or gathering and planting. As civilization expanded through commerce and trade, so too did the need for information security grow.

It was during the 1970s that information/communication security attacks first began in the emerging digital telecommunications sector. The first of these digital hackers appeared on the scene attempting to circumvent the telecommunication system and make free phone calls. This practice soon became known as "phreaking." One of the most widely known phreakers was "Captain Crunch," a.k.a. John Draper who pioneered the practice and was later arrested and convicted on charges relating to multiple nefarious phreaking activities.

As the use of personal PCs entered commercial markets in the 1980s, so too did the era of hackers who deployed malware to exploit computer systems. The first known virus, "Brain" appeared in 1986, and drove enactment of The 1986 Computer Fraud and Abuse Act, which in turn led to the first computer hacker to be

featured on America's Most Wanted—Kevin Poulson. The Brain virus was followed by the infamous Morris worm in 1988.

As computer malware blossomed throughout the 1980s, computer professionals began fighting this scourge in earnest in the 1990s by developing our modern information security industry. However, threats continue to grow during this decade which saw the birth of the Michelangelo virus, Melissa and Concept. As our computer networks increased, hackers found new, innovative ways to disrupt services such as denial of service attacks, and the introduction of bots such as Trin00, Tribal Flood network and the Stacheldracht. During this time, a host of computer frauds began to occur, as AOL suffered phishing attacks aimed at stealing users' logon information. During this time, users also saw the invention of "cookies" to track user surfing behaviours.

But it wasn't until the beginning of the new millennium that malicious Internet activity became a major criminal enterprise. Online banking came of age, as did phishing attacks targeting banking procedures and banking clients. As use of the Internet and e-commerce began to explode by 2003, there was no shortage of hackers ready to exploit opportunities to disrupt services, introduce malware and extort unwitting suspects. Adware and spyware came of age and became the bane of all computer users. Aggressive, self-propagating malware on a global scale became the new normal, as threats such as Code Red,Nimda, Welchia, Slammer and Conficker begin working your way through computer systems.

Today we see a plethora of zero day attacks, rootkits, rogue anti-spyware, SPIM, clickfraud and other attacks working your way through our devices and taking advantage of the social media craze. Even the age-old scheme of kidnapping reinvented itself on the Internet, resulting in kidnapping of persons for the white-slave trade, as well as kidnapping of your computer and data through Ransomware. Hackers have for the most part changed from small, petty disruptions, as their small time get rich quick schemes transitioned to transnational criminal organizations stealing large sums of money and millions of identities, and even further to state-on-state attacks in a quest for the highest levels of espionage and economic disruptions. Small organizations, such as terrorist organizations, have also exploited cyber breaches to provide themselves with cyber opportunities in asymmetric warfare, as they attempt to bring superpowers to their knees through disruption of commerce and attacks on communications and command and control facilities.

2. Cybersecurity Threats

Know that you are at risk! You have probably been hacked and don't even know it. If you haven't been personally cyber-assaulted, good for you! (Although I can almost 100% guarantee, if you have not been cyber-assaulted, you are about to be!) According to the 2016 Internet Security Threat Report, zero-day vulnerabilities discovered in software has increased by an alarming 125%! During the past year, over half a billion personal records were stolen or lost, while incidents that did not report identities exposed increased by 85%. What does that mean? We have probably been compromised but businesses won't admit it, as they seek to preserve their reputations. Vulnerabilities have been detected in over 75% of all legitimate websites with over one million web attacks against people occurring each day! Ransomware attacks have even begun to seize smart phones, watches, and television sets!

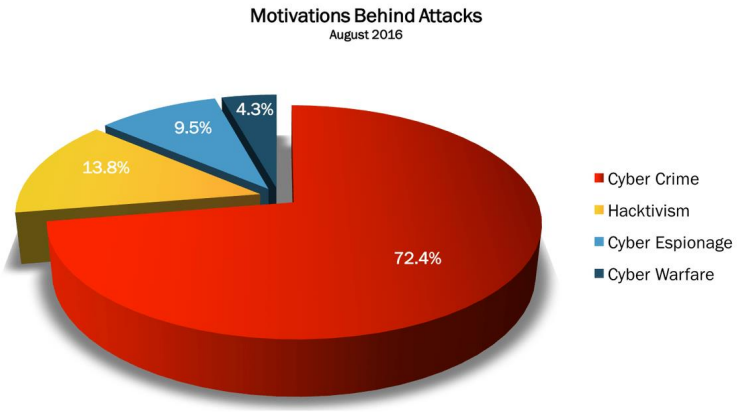


Figure 1. Motivations behind current security attacks 2016
http://www.hackmageddon.com/category/security/cyber-attacks-statistics/

To understand the threats, it is important to understand the motivation behind the attacks. Clearly, the greatest threat we face is from cybercrime, with over 72% of the attacks designed to separate a person from valued possessions for the enrichment of the attacker. Hacktivism, the act of hacking a network or system to convey a political or social message is the second largest motivator for cyber-attacks, at a distant 13%. Both cyber espionage (9.5%) and state-on-state cyber warfare (4.3%) are growing concerns.[1]

3. Essentials of cybersecurity

The key element of cybersecurity protection begins with ***people,*** as humans are the weakest link in cybersecurity chain. Everyone wants convenience and ubiquitous access, but security by definition needs to restrict those who seek to do harm to the important files and systems. The safest systems, of course, are those that are completely isolated from outside contact and not accessible online. However, even these are vulnerable if outside flash drives are connected to the system. Since most of us can't or won't put our files completely off-line we need to resort to other protective measures.

Here are some things that can be done to protect your systems.

a. Backup your files! This should be a routine part of your home cyber security process, but becomes even more important before you travel, as your data such as contacts, photos, videos and other mobile device data will be more exposed during your journey. Also, if you don't need the data, don't take it.
b. Do not connect devices to your network that have potentially been compromised.
c. Keep your antivirus software and operating systems up to date. It's vital that you keep your operating system software and applications up-to-date. This simple precaution will improve your device's ability to defend against malware and zero-day exploits.

[1] Statistics based principally upon Hackmageddon, and confirmed through statistics published by Pew Research Center, Time Magazine and other sources.

d. On mobile devices, know your applications and review their access on your device. A recent study determined that 98% of applications currently in use for our mobile devices have vulnerabilities. We often install new applications without consideration of the application's access to our location, contacts, and the capability to independently update our mobile devices. Understand that each application access point may provide an opportunity for cyber-attack.
e. Lock your device. If you are not already doing so, start the habit of locking your device when not in use. Just a few moments of an open, unattended device can give cyber thieves the opportunity they need to steal or destroy your information. Use strong pins and passwords to lock it. Considered developing a personal rubric, which is easy for you to remember, and which can be used for encrypting personal passwords. One of the most common password number sequences used on mobile devices and for credit cards is the number sequence 2580, or its reverse 0852, since these numbers are linear on our devices and easy to see and recall. Try adding a personal number to each number of the sequence and use the last digit as your new passcode. For example, if my personal number is "3" my new passcode for the sequence "2580" becomes, "5813."

4. Implications for the new decades.

The move to constant access on the Internet where all of our electronic devices are interconnected to the Internet for access and our convenience will have serious cybersecurity implications. These advanced systems, known as cyber-physical systems (CPS) are being incorporated into diverse product areas such as aerospace, automotive, chemical processes, civil infrastructure, energy, healthcare, manufacturing, transportation, entertainment, and consumer appliances.

These CPS systems are engineered from, and depend upon, the seamless integration of computational algorithms and physical components working through a communications network that will transform the way people interact with engineered systems. This new revolution will provide endless new, creative capabilities for human–machine interaction, and has already spawned the "Internet of Things" (IoT) which will transform our interactions much like the Internet transformed our interaction with information. In the very near future computer systems will replace drivers in all of our vehicles.

With the increased use of cyber-physical systems comes the increased threat of cyber security breaches.

Two things remain certain. First, systems operating on our networks will always be vulnerable to attack and must be secured. Second, our future lives will be increasingly dependent upon cyber-physical systems, making us more vulnerable. A rational approach to the purchase and use of these items, as well as required standards of performance by business and industry to mitigate the threat will be essential.

ABOUT THESE CYBERSECURITY ARTICLES

Florida International University School of Computing and Information Science (FIU SCIS) is proud to re-release this series of articles to you in hopes of providing better cybersecurity to all. These international articles in cybersecurity were published by the DECCAN HERALD Newspaper in Bangalore, India, as part of project with them in educating people to be more "cyber aware." This series of articles was written by Dr. S.S. Iyengar and Jerry Miller.

Dr. S.S. Iyengar is the Distinguished Ryder Professor and Director of the School of Computing and Information Sciences at Florida International University, where he also directs *CIERTA, the FIU Cybersecurity Center for Cyber Infrastructure, Education and Research for Trust and Assurance*.

Jerry Miller is Research Coordinator for Discover Lab at the School of Computing and Information Sciences and also an Adjunct Faculty member there, where he assists in conducting research investigations through CIERTA and the Discovery Lab in security of robotics, autonomous vehicles and cybersecurity.

The articles were published as dated and can be found at the following links.

September 14, 2016
Cyber war goes personal; monitor your online reputation
http://www.deccanherald.com/content/570208/cyber-war-goes-personal-monitor.html

August 06, 2016
Robots to counter terrorism: a brave new world?
http://www.deccanherald.com/content/562497/robots-counter-terrorism-brave-world.html

July 04, 2016
Telebot and cyber security concerns of a new future
http://www.deccanherald.com/content/555806/telebot-cyber-security-concerns-future.html

June 07, 2016
Make your travel safe, free of cyber attacks
http://www.deccanherald.com/content/550897/make-your-travel-safe-free.html

May 17, 2016
Future cyber security: smart, safe cities
http://www.deccanherald.com/content/546867/future-cyber-security-smart-safe.html

April 04, 2016
IS CyberCaliphate readying for deadly net attacks
http://www.deccanherald.com/content/538401/is-cybercaliphate-readying-deadly-net.html

March 07, 2016
Internet as the new Silk Road for the new decade
http://www.deccanherald.com/content/533037/internet-silk-road-decade.html

February 4, 2016
The Darknet, cyber secrets and concealing identity

http://www.deccanherald.com/content/526816/darknet-cyber-secrets-concealing-identity.html

December 31, 2015
The future of learning: Hack-a-thons and cyber learning
http://www.deccanherald.com/content/520545/future-learning-hack-thons-cyber.html

December 3, 2015
Biometrics and digital forensics: Cyber security connections
http://www.deccanherald.com/content/515241/biometrics-digital-forensics-cyber-security.html

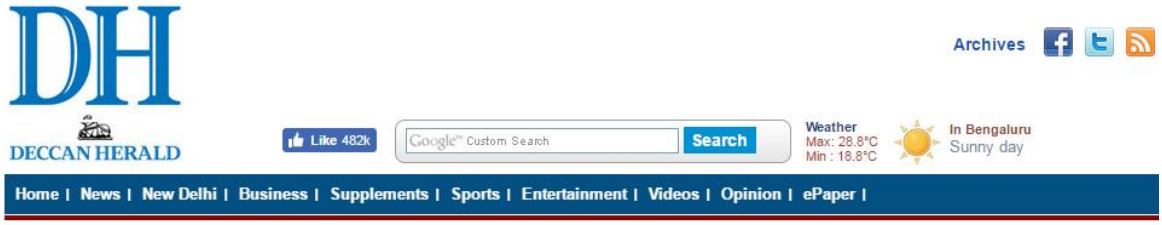
November 5, 2015
Cloud computing good, but it can be dicey too
http://www.deccanherald.com/content/510176/cloud-computing-good-can-dicey.html

October 02, 2015
Cyber-physical systems will be future driver of your car
http://www.deccanherald.com/content/503998/cyber-physical-systems-future-driver.html

September 7, 2015,
Big Data and Cyber Security: What have you given away?
http://www.deccanherald.com/content/499490/big-data-cyber-security-have.html

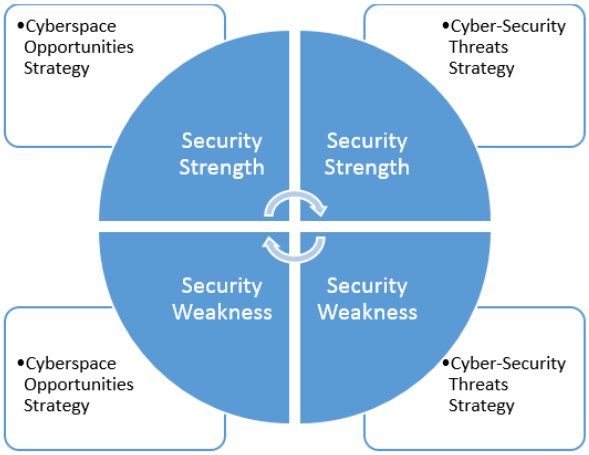
August 10, 2015
Roots of modern 'cyber' terrorism in a divided world
http://www.deccanherald.com/content/494314/roots-modern-cyber-terrorism-divided.html

July 24, 2015
Cyber security: Are secrets possible anymore?
http://www.deccanherald.com/content/491073/cyber-security-secrets-possible-anymore.html



CYBER WAR GOES PERSONAL; MONITOR YOUR ONLINE REPUTATION

By S S Iyengar and Jerry Miller, Sep 14, 2016



Recently, an online retail company sold a bad yo-yo to a teen-aged customer. After several lengthy go-rounds from the teen requesting a return of the product and a refund, the company dismissed the customer, failing to live up to their written, contractual obligations, and leaving behind an extremely disgruntled former client.

In the past, companies could have easily written off a scenario like the one above, as "just one unsatisfied customer" which they might suspect would not disrupt much of their business. Oh sure, occasionally you get the customer who will threaten to take you to court, but the company legal team usually gets by this in, dragging out the legal process until the angry customer can no longer afford to fight the battle. Today, however, this is no longer the case.

A day later, the CEO awakened to a nasty surprise, when his CIO reported that the company website had been taken down by someone or something, such as a bot (web robot), or software application that runs automated tasks over the Internet with extraordinary fast speeds. The bot was the lead agent in a devastating attack on the company. Soon thereafter, a directed denial of service attack flooded the company servers, crashing their systems and taking their business off-line.

When the company recovered from this attack, they soon discovered thousands upon thousands of bad blog posts, smearing the name of the company. Bad reviews on the company were soon coming in from across the globe.

Additionally, company websites and emails were laden with malware and Trojans. Within days, company sales had deteriorated to nothing. Social media sites such as Facebook and twitter were abuzz with word of the demise of the company, its poor service, and complete disregard for customer service.

A few weeks later, the company did indeed fail. While this scenario is fictitious, companies around the globe are now facing real-time threats from disgruntled customers and employees. The Internet is enormous, and

for those who disregard it, the Internet can become an extremely hostile place to a company's reputation, and future prospects. It can be the end of your bottom line—both personal and professional.

It's as important to understand and monitor your online reputation, as it is to install critical firewalls and antivirus protections both at home and in the workplace.

Management and control of cyber security is entirely yours. No one else can assess your needs, your use, and ultimately your safety on the Internet and in social media. Although experts are available to help, implementation is based upon behaviours within the company coming directly from each employee.

As the Internet continues to expand, so too does social media, the cloud and our need for mobility with the "bring your own devices" invading every workspace. With the advancement of artificial intelligence and autonomous computing, the world has become a very interesting and dangerous place. Loss of personal privacy is becoming commonplace as we freely give away our information for the use of social media platforms and applications that now track our every move. With access to this information, the loss or defacement of an online reputation can come quickly and stay permanently.

Many of us have hundreds of friends on Facebook, and hundreds more of professional associates on media groups such as LinkedIn. But how many of these "friends" and "professional associates" do we really know personally? Would any of these "friends" and "professional associates" be potential enemies, turning against you to destroy your online social reputation?

Florida International University is conducting interesting research in a variety of aspects of social media to answer these and other questions that pertain to your online loss of privacy and potential violations of your personal security.

While we cannot give you a one-size-fits-all shield to protect your loss of privacy and manage your social media reputation, we can offer some suggestions for safer and more productive experiences.

Some suggestions

From our research, we offer the following suggestions:

1. Conduct an internal Strengths, Weaknesses, Opportunities and Threats (SWOT) analysis of your cyber business and personal life. Identify those things that are working for you, such as your firewalls, anti-virus software, virtual private networks, and other security practices/procedures and keep assessing their effectiveness. Determine weaknesses and vulnerabilities in your security practices, as well as the way you do business online, how your employees interact across the Internet, the devices they bring into the workplace and the potential for transfer of viruses onto your network systems. Also assess the way you access and use social media. Identify potential new opportunities, but keep in mind that competition has the same aims and may implement counter social media systems that become a threat to your business or personal life.

2. Develop an internal policy with access control lists—who and what apps can have access to your personal information. Beware of both lazy and bad people. Many times, malware can be installed on your equipment because either you or your people were lazy and not attending to the security and privacy settings on your

systems. Never let anyone else use your login credentials. If login credentials are compromised, immediately change your login information.

3. As regards “bad people,” there are those who have no morals or ethics and could at any time turn from friend to enemy. Beware! This could include social media contacts, email clients who are phishing, and even you when you post stupid pictures of yourself on a website. Remember, once something is on the Internet, it’s out there forever!

It’s important to check your digital reputation regularly, to determine if someone has “bombed” you in the social media. Be careful out there...the Internet can be a jungle!

ROBOTS TO COUNTER TERRORISM: A BRAVE NEW WORLD?

S S Iyengar and Jerry Miller, August 06, 2016

O wonder!
How many goodly creatures are there here!
How beauteous mankind is! O brave new world, That has such people isn't.
— William Shakespeare, The Tempest

It is indeed a brave new world. The irony of the statement by Shakespeare's character Miranda has been captured many times over as technology advances both in tune with technology, and while simultaneously warning against these advances. We find ourselves immersed in the same debate today, as we consider artificial intelligence (AI) and its potential use in "Killer Robots."

As early as 2009, organisations began calling for a pre-emptive ban on killer robots, when the International Committee for Robot Arms Control (ICRAC), founded by roboticists, ethicists, and others, issued a call to stop AI research that could lead to development of killer robots. Five years later, the European Parliament passed a resolution calling for a ban after more than 20 Nobel Peace Laureates issued a statement in favour of banning the robot.

In the Third Convention on Conventional Weapons (CCW) held in Geneva from April 11 to 15, 2015, two high-ranking UN experts issued a report to the Human Rights Council calling for a moratorium on autonomous killer robots. By July 2015, the Future of Life Institute issued an open letter which more than 1,000 AI experts signed supporting a prohibition. Today, there is an active Human Rights Watch campaign to ban the development and use of these technologies.

But are they fighting to turn back time? In 1863, English author Samuel Butler published an article, "Darwin among the machines," arguing that "the machines will hold the real supremacy over the world and its inhabitants," and further arguing that as a precaution, humans should return to the "primeval condition of the race." Earlier, the Luddites ravaged English factories, destroying machines they feared were threatening their jobs.

In the 17th century, during a period of intense seclusion, the Japanese went so far as to outlaw the use of firearms, which had been introduced into the country as early as 1270 from China, only to resume their use during the conflicts of the mid-1800s.

Over the past few days, events in the United States demonstrate the short-sightedness of these actions while illustrating the benefits of the use of robots for law enforcement. After an intensive 45-minute shootout in Dallas,

Texas, USA, two police officers lay dead and three others would die within hours from massive injuries received at the outset.
An assassin was targeting police officers and terrorising a major US city. Police began negotiating with the sniper to no avail. After two-hours of intensive negotiations, the Dallas chief of police gave an order to neutralise the suspect by any means without risking more officer's lives.

The plan was ingenious. The SWAT team called upon the RemotecAndrox Mark V A-1 robot, manufactured by Northrup Gruman, to deliver a pound of high explosive C-4 directly against a wall on the second floor of the building behind which the sniper was cowered.

The robot delivered its payload, completing its mission with only minor damage after the explosive charge ripped a hole in the wall, fragmenting the sniper. This ended the standoff and officially introduced robots as an anti-terrorist weapon.

Robots can be mounted with a variety of sensors and tools for law enforcement. The A-1 generally carries a flashbang, a device that emits a bright light and loud sound to stun criminals. These robots can also place an explosive near a bomb in order to disarm it through the explosive discharge. But there are far more uses for the robot, as outlined on Northrup Grumman's Remotec website based upon an assortment of accessories available.

The robot can be affixed with a modified 12 gauge shotgun, which can also be used as a breaching tool; a gas can dispenser mount; a window breaker, a cable cutter; a variety of drills and saws, as well as real time x-ray machines, or mounts for the weapons launcher.

Innovative new uses

Interestingly, Northrup Grumman lists the Remotec Androx Mark V A-1 robot as, "ready to handle any situation at a moment's notice." Thankfully it was ready when called upon. Police departments across the United States, and around the world, are procuring the next generation of robots to make law enforcement safer, as criminals and terrorist employ innovative new uses for common items, such as passenger aircraft and explosives.

One of the largest robots currently in the field is the BatCat—a 39,000-pound remote controlled vehicle used to lift cars, and tear into buildings, or barricaded areas. The BatCat (Bomb Assault Tactical Control Assessment Tool) is built upon Caterpillar's Telehandler base and comes equipped with claw, forklift, and/or bucket in order to make a dynamic entry or respond to improvised explosive devices on vehicles.

On the small end is the Recon Robotics Throwbot, which can run slightly ahead of a clearing team to provide valuable intelligence and pictures of potential threats. Weighing just 1.2 pounds, Throwbot can be thrown up to 120 feet (36m) in front of a police team. Directed by an operator receiving audio and video, Throwbot can also transmit infrared optical data of its surroundings.

Autonomous and semi-autonomous robots are already involved in a multitude of missions against terrorists and criminals alike. Our safety, as well as that of the men and women who serve us in law enforcement, depends even more on the tools available to outwit the evil that surrounds us.

While we accept the fact that technology must advance, we also must accept that all technologies can be used for both good and evil. We are a long way from autonomous robots using artificial intelligence to destroy humankind. At Florida International University (FIU) Discovery Lab, we are exploring robots for many real-time applications.

DH
DECCAN HERALD
Archives
Like 482k
Google™ Custom Search
Search
Weather
Max: 28.8°C
Min : 18.8°C
In Bengaluru
Sunny day
Home | News | New Delhi | Business | Supplements | Sports | Entertainment | Videos | Opinion | ePaper |

TELEBOT AND CYBER SECURITY CONCERNS OF A NEW FUTURE

S S Iyengar and Col Jerry Miller, July 04, 2016

The field of robotics has expanded enormously in the past two decades and will continue to do so far into the foreseeable future. Stationary, industrial robots are now incorporated in nearly every aspect of manufacturing and assembly line production where they are used to cut and mould parts, conduct inspections and assemble pieces.

Mobile robots have been developed to conduct tasks in environments which could expose humans to a variety of risks such as inspections in industrial areas handling hazardous chemicals, potential nuclear radiation leaks, and deep underwater marine environments. Other areas in which robots may ultimately provide significant assistance in protecting humans from risks to their health and well-being include conducting humanitarian and disaster relief operations.

The United States Defence Advanced Research Projects Agency (DARPA) has for several years now conducted robotics challenges to promote innovation in human supervised robotic technology for disaster response operations. The DARPA's stated technical goal for these robotic competitions is, "…To develop human supervised ground robots capable of executing complex tasks in dangerous, degraded, human-engineered environments." These robots are required to use standard tools and equipment such as hand tools and vehicles currently employed by humans to conduct these disaster operations.

Robots have even expanded into space exploration. The US National Aeronautics and Space Administration (NASA) has begun testing robots for use on future moon and mars explorations. These tests are essential in assessing new ideas for rovers, spacewalks and ground support vehicles in remote, hostile environment such as deep space, where temperatures, as well as surfaces can be extreme.

However, one of the most important expanding areas for the use of mobile robots is the use of semi-autonomous robots for military and law enforcement activities. While scenarios such as inspection of hazardous areas and monitoring of barricaded suspects, or serving high risk warrants have been considered for law enforcement, by far the most common use of robots in military and law enforcement activities to date has been in the area of bomb disposal.

Other scenarios for robots have included reconnaissance in tunnels and storm drains, as well as surveillance at airports and seaports, conducting searches for criminals and lost persons, providing site security, and use

as a public reception and information dispenser. Each of these robots is specialised to perform their current tasks.

Florida International University's (FIU) Discovery Lab, a research lab within the School of Computing and Information Sciences (SCIS), has been conducting research into the use of a fully integrated, telepresence robot to act as an avatar for injured law enforcement officers. Student researchers under the guidance of faculty mentors have created a six-foot tall, 80-pound life-sized avatar to conduct a variety of law enforcement activities.

The robot, known as "Telebot" is a telepresence robot which uses video cameras for its eyes, as well as an integrated sonar in its nose to detect and focus its eyes on the presence of both obstacles and people in its path. Telebot is also equipped with a voice command system, enabling the robot to speak and to listen for commands, as well as inte-ract with the public. Operated and controlled remotely by a law enforcement officer, Telebot enables an injured law enforcement officer to continue to perform their duties.

Telepresence robots

Currently, when a law enforcement official is injured in the line of duty, with a prolonged outlook for medical rehabilitation, or if an officer is unable to meet previous physical fitness requirements, the officer is medically retired, ending both the officer's career, and the community's access to the officer's vital experience. This is often devastating news to the officers, who lose not only their livelihoods, but also their self-esteem.

Telepresence robots, the new future for law enforcement, will allow these officers to continue to serve in a capacity where their wide and varied experience can be used most effectively in a complete array of community service. Using a variety of sensors to detect inputs from the controlling officer, Telebot is able to respond and act on behalf of the officer. In addition, Telebot is a semi-autonomous robot with artificial intelligence, meaning that he not only responds to commands and controls from the disabled officer, but can respond to threats, obstacles and people within its deployed environment and learn on its own.

This provides protection for the Telebot, as well as people and property within its path, or around it. For example, if a young child should approach Telebot from behind, while its video vision and hence the operator's vision is focused to the front, sensors will warn Telebot about the approaching child, so he does not inadvertently swing an arm in the child's direction and injure the child. As humans, we sometimes sense that someone is approaching us from the rear or side, but too often, our senses fail and we turn into the person knocking them, or ourselves to the ground.

Hollywood movies have highlighted the potential for evil runaway droids to use their autonomy and artificial intelligence to take the law into their own hands. However, these scenarios are far-fetched. But they do highlight the need for integrated cyber security to prevent evil humans from creating havoc by taking control of semiautonomous robots.

Obviously, the vast array of sensors and sensor systems incorporated into Telebot are susceptible to the same cyber security concerns as other devices working across the Internet. To prevent disruption of service, researchers are integrating advanced cyber security designs into the software and hardware controllers, as

well as signal transmission and reception components for Telebot. Both telepresence robots and cyber security will continue to advance and integrate rapidly. In the near future our world may become a safer place due to deployment of robots like Telebot.

DH
DECCAN HERALD
Archives
Like 482k
Google™ Custom Search
Search
Weather
Max: 28.8°C
Min : 18.8°C
In Bengaluru
Sunny day
Home | News | New Delhi | Business | Supplements | Sports | Entertainment | Videos | Opinion | ePaper |

MAKE YOUR TRAVEL SAFE, FREE OF CYBER ATTACKS

S S Iyengar and Jerry Miller June 07, 2016,

Travel is among life's greatest pleasures, but it can also become a horror story if the traveller is unprepared. A few simple, preparatory steps before your journey combined with knowledge and vigilance during your trip can make the difference between a pleasant experience and a personal or professional cyber disaster.

Preparation is the key. While the cyber security basics practiced at home will be the same during your journey, travelling does open up new opportunities for cyber-attacks, cyber theft and loss, or compromise of personal devices. Make a quick reviewing of your cyber security procedures, then expand on them by conducting a quick risk assessment using these questions.

What information will I be carrying with me that will need to be protected? This is an important item to consider if you will be travelling for business and have sensitive client information with you, including names, addresses, phone numbers, business account numbers and credit card numbers.

Consider storing important data separately on a CD, or USB device, then keeping it in a separate location apart from your laptop or mobile device. Should physical theft occur, thieves would not have access to your sensitive, protected information.

Should I encrypt sensitive files? Encryption safeguards data from unauthorised access even if the information is stolen. However, encryption can be a double-edged sword. If you forget your encryption password, you will not be able to access your data.

Do I have an inventory of all my mobile devices and equipment to be carried on my journey? Mobile devices and laptops should be physically carried with you and not placed in unaccompanied baggage, where it is a target for either physical or cyber theft. Know what you have so you leave nothing behind in hotels, at airports, or in public transportation.

Be sure you take actions outlined in the following steps in addition to correcting any of the risk items that you may have noted.

Update software on your mobile devices. We are often quite diligent about maintaining antivirus software on our desktop and laptop computers, but often forget about our mobile devices. It's vital that you keep your operating system software and applications up-to-date. This simple precaution will improve your device's ability to defend against malware.

Know your applications and review their access on your device. A recent study deter-mined that 98% of applications currently in use for our mobile devices have vulnerabilities. We often install new applications without consideration of their access to our location, contacts, and the capability to independently update our mobile devices. Understand that each application access point may provide an opportunity for cyber-attack.

Backup your information. This should be a routine part of your home cyber security process, but becomes even more important before you travel, as your data such as contacts, photos, videos and other mobile device data will be more exposed during your journey. Also, if you don't need the data, don't take it.

Lock your device. If you are not already doing so, start the habit of locking your device when not in use. Just a few moments of an open, unattended device can give cyber thieves the opportunity they need to steal or destroy your information. Use strong pins and passwords to lock it. Considered developing a personal rubric, which is easy for you to remember, and which can be used for encrypting personal passwords.

One of the most common password number sequences used on mobile and for credit cards is the number sequence 2580, or its reverse 0852, since these numbers are linear on our devices and easy to see and recall. Try adding a personal number to each number of the sequence and use the last digit as your new passcode. For example, if my personal number is "3" my new passcode for the sequence "2580" becomes, "5813."

With our preparations complete, and our mobile devices in hand, it's time to start our journey. Remember your smartphone, tablet, or other mobile device is a full-fledged computer, and must be treated with even more concern for online risks in shopping, banking, enjoying social media, or sharing personal information online. Be diligent! You are now dealing with both physical and cyber security concerns.

Wi-Fi networks
Public Precautions. Avoid using open Wi-Fi networks to conduct personal business, banking, or online shopping. Open Wi-Fi networks enable attackers to intercept sensitive information. If it absolutely must be done, turn off your device's Wi-Fi and use the cellular data connection instead, as this provides far more security than open access, unsecured Wi-Fi networks.

Turn off Bluetooth enabled accessories. While Bluetooth devices can be helpful, cyber criminals have the capability to pair with your device and steal personal information. Public charging of your device can also lead to a compromise of data. If you connect to a public charging station such as those provided at airports, it is possible that the USB cable can allow software running on that system to enter your device, gain access to your information, or install malicious software. Carrying your own external battery charger is the safest way to go.

Be vigilant when logging into devices in airports, hotels, or public transportation. Guard your username and password from view. Also, safeguard your laptop securely when not in your hotel room. Never leave your laptop running in the room, even if you depart for only a few minutes. Thieves may have access to the room and could quickly connect and download your data.

Also remember to safeguard your boarding pass to prevent access to personal information within the barcodes. By observing a few key precautions, and maintaining vigilance, you'll be able to delight in your journey. Bon voyage!

DH
DECCAN HERALD
Archives
Like 482k
Google™ Custom Search
Search
Weather
Max: 28.8°C
Min : 18.8°C
In Bengaluru
Sunny day
Home | News | New Delhi | Business | Supplements | Sports | Entertainment | Videos | Opinion | ePaper |

FUTURE CYBER SECURITY: SMART, SAFE CITIES

S S Iyengar, Col Jerry F Miller, May 17, 2016

Since time immemorial, people have flocked to cities seeking economic advantage and safety. However, as populations grew, it became difficult for people to find either. Cities and their resources have been stretched to their limits by exponential growth, the boom and bust cycle of business and by crime.

Natural and man-made disasters also impact an increasing number of people and their safety. It's been reported that 31% of India's population now lives in cities, where they generate 63% of the nation's economic activity. City growth in India is projected to increase at a rate where over half of the population will be urbanites by 2030.

Recent technological advances, in particular the use of sensors, mobile devices and online social networks have inspired a revolution in city design and management which have led to the development of smart cities.

Through the Smart Cities project started by Prime Minister Narendra Modi, India recently launched three enormous urban schemes to improve living conditions in cities – the Smart Cities Mission, Atal Mission for Rejuvenation and Urban Transformation (AMRUT), and Housing for All in urban areas. The Government of India allocated Rs 98,000 crore to develop 100 smart cities over the next five years.

What are Smart Cities?: "Smart City" is the buzzword for a new or revitalised urban area integrated with multiple secure information and communication technology (ICT) solutions to manage the city's assets, including education, transportation, electrical, telecommunication, waste management as well as health and safety systems. Innovative ICT is at the heart of this revolution in city planning. Through the use of sensors integrated with real-time monitoring devices, important infrastructure systems data are collected and analysed to improve efficiency, reduce costs and ensure supply and use of sustainable resources.

Education is an important core element of a smart city programme. In order for these programmes to work and be effective, people need to understand what smart systems are and how they can participate in their use and drive their development to assist them in their daily lives and businesses. An understanding of the value of different smart systems will also lead to an understanding of the challenges of privacy, ethics and security inherent in all digital information collections and analytics.

Utilities comprise some of the first and most important elements of a smart city's infrastructure. Utilities companies have installed smart metres that not only record the overall amount of energy used, but can be

programmed to record every half hour or less at home in order to precisely determine energy consumption, notify the utility of a power outage, and allow the company to remotely switch electricity service on or off to a particular building, saving time, resources and manpower. Data collection and analysis through these digital metres enable energy providers to be more efficient and to calculate exact times when energy demands may be highest for particular regions.

Improved efficiency

The use of smart systems in transportation has demonstrated improved efficiency in travel and parking. Through the Florida International University Smart Wave Project in Miami, Florida, the US, researchers have been working with the National Science Foundation and the Florida Department of Transportation to develop improved transportation systems for Miami and other major global cities.

All systems developed, demonstrated and validated through this research incorporate a smart vehicle component using the Informed Traveller Programmes and Applications (ITPA) technologies. The ITPA provides an informed, multimodal travel system using real-time, travel related data on present traffic flow, emergency events, special community events, weather, historic traffic affecting trends and parking conditions at an informed traveller's destination. The information is presented on a smartphone-based interface that provides personalised, timely information and advice. The system provides the most efficient, cost-effective travel paths for users consistent with the traveller's destination and scheduling requirements.

The system is in use at Florida International University in Parking Garage-6, known as the Tech Station. Through a variety of sensors, the system monitors all parking spaces and relays open parking information to travellers as they arrive at the university. Through their smartphone interface it directs them directly to the specific open parking area to their destination, saving time and fuel.

Within the School of Computing and Information Science at Florida International University, researchers including the author, have developed a smartphone-based system known as iSAFE, which provides a personalised, context aware safety programme that analyses and predicts crime throughout an urban area such as Miami, and relays the information to the user as he travels through various communities within the greater urban area.

The device computes real-time snapshots of the safety profiles of users in a privacy preserving manner. By dividing the entire urban environment into small census blocks and evaluating them through time periods based on types of crimes committed, such as homicide, larceny, robbery, assault etc., the system can actively advise a traveller when he is approaching a potentially hazardous area at that particular time. The system continues to provide information to predict the area's crime index, identifying potential alternate routes for the travellers, which provide better personal safety.

The ITPA, iSAFE and other systems can be applied to health, medical and other individual systems to provide predictive safety, security and public health to inhabitants within our smart, safe cities. As we continue to advance these technologies, researchers are incorporating cybersecurity to ensure these systems remain uncompromised.

DH
DECCAN HERALD
Archives
Like 482k
Google™ Custom Search
Search
Weather
Max: 28.8°C
Min : 18.8°C
In Bengaluru
Sunny day
Home | News | New Delhi | Business | Supplements | Sports | Entertainment | Videos | Opinion | ePaper |

IS CYBERCALIPHATE READYING FOR DEADLY NET ATTACKS

S S Iyengar and Jerry Miller, April 04, 2016

On March 22, 2016 just before 8 am local time in Brussels, two horrific explosions shredded its busy airport departure area. Shortly thereafter, another bomb ripped through a subway station in the city marking the deadliest assault on European heartland since the Islamic State's attacks on Paris four months ago. At least 30 people were killed in the Brussels attacks.

Shortly thereafter, the IS claimed responsibility for the attacks, in their growing, global strategy against the influence of the Western nations. Their message, claiming responsibility for the attacks was clear, "We are promising the crusader nations which have aligned themselves against the IS that dark days are coming." Since January 2015, they have organised a consistently brutal series of attacks targeting civilians and carried out by a network of terrorists and sympathisers linked to or inspired by IS.

The terror group organised and directed an assault across Paris that killed more than 100 people. The attacks on Brussels appear to be a continuing outgrowth of the Paris attacks. All in all, IS has been responsible for more than 35 physical, land domain attacks around the world. But IS has not been confined solely to the land domain. While their efforts have not and yet been observed as attacks in the domains of space and sea, their battles have already incurred casualties in two domains—land and air.

In October 2015, it downed a Russian passenger jet killing 224 people, extending their conflict into the air domain. By building relationships with jihadist groups that can carry out military operations throughout West Asia and North Africa, they have expanded their reach and have declared provinces in Nigeria, Algeria, Libya, Egypt, Syria, Iraq, Saudi Arabia, Yemen, Afghanistan and Pakistan. Who will be next?

War is much like a fire where there are four critical elements. In a fire, the elements are a fuel source, oxygen, and a spark, as well as a critical fourth control element, the environment that fosters (or limits) the expansion of the flame. In war, there are also four critical elements, comparable to that of a fire, namely, material, manpower, and leadership, as well as the fostering or limiting environment (the domains of land, sea, air, space and cyber). In the terrorism game, bomb building explosive materials, as well as computer systems are some of the "war materiel" providing fuel for the fire.

Manpower, much like oxygen with fire, sustains the combustion. In the terrorism game, without manpower, sustaining the ideas and the enthusiasm of the ideology, the efforts would soon die out. After all, with each new bomber willing to destroy themselves in the name of jihad, another must be found and trained or you will quickly run out of suicide bombers to throw at your enemies. The spark of course that ignites the fire is the leadership, especially those skilled in the art of planning, communicating, bomb-making and the use of information and computers.

The environment of course is the area that limits whether the fire burns out of control or is contained in a particular region. While a fire can quickly start in an enclosed container, the enclosed container provides the environment that shapes and ultimately stops the fire before it becomes a conflagration. Place the same combination in a forest, where material is readily available with plenty of the oxygen and in an uncontained environment where the winds whip the fire across natural and man-made breaks, and soon the fire spreads completely out of control.

Cyber methodologies

Those unfamiliar with the spread of terrorism and their adaptation of cyber methodologies might ask, "What role are the terrorists playing in cyber?" The answer is they are playing a significant role with the advent of the CyberCaliphate. They are using cyber to recruit new members and provide the fuel that fires their jihad. They have also begun to expand their use of cyber beyond recruitment, and into the realm of cyber-attacks against their enemies, through the CyberCaliphate.

The CyberCaliphate is cyber jihad where the medium, platform and social connections promote cross-media horizontal dissemination and global amplification of the digital media. Knowledge is power.

The IS understands the role of the fifth domain—cyber—and is attempting to control the domain to their advantage. It is using Twitter, Facebook, YouTube and Vine, as well as other social media platforms to "transform the medium itself into a weapon" where speed of use and portability transforms their terrorist message into a ubiquitous presence, continuously reminding their enemies of their potential to strike.

The group has hacked more than 54,000 Twitter accounts initially in retaliation for a drone strike that killed their British member in November 2015. CyberCaliphate seized control of accounts and used them to spread the IS propaganda.

The group published details of most of these 54,000 Twitter accounts, including passwords and mobile phone numbers, as well as other personal information. Their victims include members of the United States CIA, FBI and National Security Agency. Right before their victim's eyes, the group seized their accounts and posted IS propaganda in their Twitter accounts while the victims could only watch in horror.

This cyber army also announced plans in early January 2016 to hack Google. Fortunately, Caliphate Cyber Army (CCA) has so far not been able to do that. Claiming victory against Google by hacking their site, the CCA posted evidence of their success. Unfortunately for them, the website http://addgoogleonline.com, which was registered in the name of Gandani K in India, was not a Google site, so Google remained unscathed.

However small the CCA's victories appear, the United States government has taken notice. On February 29, 2016, US Defence Secretary Ashton Carter declared a cyber war against the IS acknowledging that the US Cyber Command has begun facing off on the virtual battlefield against the jihadi cyber terrorist.

Carter stated, "we're trying to both physically and virtually isolate IS, limit their ability to conduct command-and-control, limit their ability to communicate with each other, limit their ability to conduct operations locally and tactically." How effective this operation will be remains to be seen.

INTERNET AS THE NEW SILK ROAD FOR THE NEW DECADE

S S Iyengar and Jerry Miller Mar 07, 2016,

The ancient Silk Road, a network of trading routes that extended more than 4,600 miles, provided a conduit for trade extending from eastern China West to the Mediterranean, with departure points into Asia, India and eventually connecting maritime routes throughout the region.

The term Silk Road, has become a metaphor for the exchange of knowledge, ideas, technology and cultures, in addition to its primary purpose of enabling caravans to exchange tangible goods, including finished products and raw materials. The Silk Road provided the principal thoroughfare for trade and the linkage between the cultures of East and West from 600 to 1200 AD. Portions of the Silk Road are still in use today.

The Silk Road became the most important access route in globalising the ancient world. The thoroughfare enabled merchants, pilgrims, soldiers, explorers, and those interested in adventure the opportunity of a lifetime. Raw materials and finished products were moved in relay fashion from city to city, and while many objects made the entire journey, few people did, as they would traditionally move from city to city and then pass on their goods to other merchants who would continue to move them along the road in a relay fashion.

Ultimately, because of their capacity to transport larger quantities and heavier goods faster than a caravan, maritime trade routes reduced or replaced the traditional Silk Road caravan routes. However, the Silk Road's impact on globalisation through the spread of music, religion, culture, and technology such as grape wine making, not to mention the use of paper money, and of course the most coveted commodity, silk, provided the basis for our modern civilisation.

Today, the Internet provides our new Silk Road for globalisation with many remarkable similarities to the ancient Silk Road. Like the Silk Road, the Internet provides an interconnected network for the transfer of goods, services, raw materials and finished products.

Just like the relay system for cargo on the Silk Road, today information packets pass from city-to-city, point-to-point across the Internet. The Internet provides us with the world's largest global bazaar, where everything is for sale. Even money as we know it has morphed into bit coins as a form of international Internet exchange. But what do you really know about the ancient Silk Road and its similarities to the Internet of today? Follow along as we explore the modern Internet Silk Road.

Today, we measure the new Silk Road not in miles, continents, or ocean crossed, but in petabytes, exybytes, of information streaming around the globe. As of February 2016, the indexed pages of the Internet are estimated to be 4.83 billion pages. If we assume the indexed pages account for only one-third of the total pages we can estimate over 14.4 billion pages are out there. These new "miles" represent a global network that spans continents and cultures.

You can now access webpages in all languages through on-line translators, as well as shop across the globe. Clients in India and China can now order items from Amazon and other vendors and have them delivered in record time.

Services can occur around the globe through Internet interactions and global stock prices affecting the markets day and night. Your airline and train boarding passes can now provide you easy access as well through the new Silk Road. You can print your pass early for your arrival and departure, quickly scan it through the checkpoints and enjoy hassle-free travel.

Secured info

The scanned information has your name, flight information, class of passage (economy, business or first class), who purchased the ticket for you and most importantly, your airline preferred customer number, which if compromised can allow access to much more information, including previous flights and destinations. By knowing your routes, destinations, and economic status, attackers can target you for kidnapping or fraud.

It is important that this information be secured when travelling. Do not leave the paper copy in seat backs or magazines, nor should you dispose of these items anywhere near the airport or train station. It is best to shred the ticket stubs when no longer needed.

There are some countermeasures that are being developed to help protect you from this type of attack. Devices are being developed to provide a code to all prospective travellers and being tested for robustness. These encrypted codes can be used like a credit card when passing through the ticket counter, minimising danger of exposure. There are some limitations to this method, as it may be difficult for older members to recall the access codes for these cards. However, through advanced biometric recognition, these access cards can be significantly improved.

These are some real threats on the Internet. At Florida International University's Discovery Lab, teams of students and rese-archers are progressing to deliver advanced biometric techniques and digital analysis of palm prints, finger prints, facial recognition software and even motion, such as walking and swiping your cell phone. All of these methods have been tested in conjunction with the telepresence robot for law enforcement. Some additional details are available on the FIU Discovery Lab webpage.

Right now there are over 1.9 billion devices connected to the Internet with an expected growth rate that will enable over 9 billion connected devices to exchange information by 2018. Future new "Silk Road" travellers will continue to enjoy opportunities for access to exciting new and different cultures. But the dangers of the Internet, are perhaps even more dangerous than along the ancient Silk Road. Let the traveller beware!

DH
DECCAN HERALD
Archives
Like 482k
Google™ Custom Search
Search
Weather
Max: 28.8°C
Min : 18.8°C
In Bengaluru
Sunny day
Home | News | New Delhi | Business | Supplements | Sports | Entertainment | Videos | Opinion | ePaper |

THE DARKNET, CYBER SECRETS AND CONCEALING IDENTITY

S S Iyengar and Jerry Miller, February 4, 2016

There has been a lot of publicity recently concerning the illegal use of the Internet. "Darknet" market sites such as Silk Road, Silk Road 2.0, Silk Road 3.0 and Silk Road Reloaded have been brought down or targeted by the law enforcement authorities. What is Darknet, why does it exist, and why are its sites often associated with the ancient Silk Road?

The Internet might be compared to an iceberg, where the top one-third is out of water and clearly seen, while the remaining two-thirds are submerged. The top, visible portion of the Internet is known as the "open web." Our search engines, such as Google and Firefox, have indexes to its sites and can lead us across the open network. For most of us, the open web is the Internet. However, the vast majority of Internet web pages are invisible to most Internet users.

The remaining two thirds of the Internet sites are "submerged," or concealed. These concealed segments are known as the "Deep Web" and the "Dark Web," or the "Darknet." They are accessible, but hidden from most users. These layers have been developed by technologies that allow Internet users to have anonymity on the web. They legitimately help individuals and companies to protect their security and privacy, and in many cases serve to protect users from censorship.

The majority of pages residing in these layers are personal or corporate pages, administrative databases, or personal photo collections. Only a very small portion of the sites in Deep Web use sophisticated anonymity systems, allowing operators to conceal identities and operate criminal activities.

While there are many legitimate reasons an Internet user would wish to hide their identity, a majority of those who do so take simple measures such as using pseudonyms on social media sites, clearing the web browser history from their computer after use, or using unsophisticated encryption methods.

Users who do not use some type of anonymity protecting measure should be aware of how easily online activities can be tracked and identities revealed. Websites and emails can be monitored and, unless encrypted, reveal vital information that violates user privacy.

Anonymity on the open web: Before a device can use the Internet as a highway for information, it requires an Internet Protocol address, or IP address, which can be recorded and often linked to individual users. However, some routers use Network Address Translation protocol, or NAT to assign a single IP address to the router and mask the multiple, individual devices on a particular local area network (LAN). If you use a wireless router to connect your devices, you are probably using this technique.

Virtual Private Networks (VPNs) provide anonymity and protection by "tunnelling" and encryption. Tunnelling establishes a "covered" communication network route which isolates the transmission.

When penetrated, it redirects and re-establishes the tunnel along another line of communication. Should the message be intercepted, it is also encrypted so the interloper will be unable to read the contents of the transmission. The disadvantage of the VPN is that a single entity (the provider of the service) has access to the identity of all users and their communication partners.

The other, more robust anonymity systems offer stronger protection. The most popular anonymity system is known as "Tor." Originally developed as a research project in 1995, Tor became operational in 2003 and has been maintained and improved by Tor Project Inc. Tor conceals a user's data within the Tor network, hiding the user's IP address and other identifiers from the websites they visit, thereby disguising the users' online activities.

Internet communication

Anyone monitoring Internet communication will find it extremely difficult to trace these activities back to a specific user. Tor's popularity stems from its ease of use, as one does not need a detailed knowledge of computers to use the system.

Tor's benefits enable anonymous use of the open web using the Tor browser, and anonymous publishing of web services as part of the Tor Hidden Services.

Tor enables users to access the open web and circumvent censorship, anonymously participate in activism and journalism, provide undercover online surveillance of specific websites, protect personal security and privacy, and anonymously conduct peer-to-peer file sharing.

Delving deeper on to the Darknet, users link to Tor/onion sites, which are part of the Tor Hidden Services (THS) network. Because THS addresses end with ".onion" rather than traditional "co.in" addresses, they are commonly referred to as "onion addresses." The THS sites are not indexed by common search engines, such as Google and Bing, making them more difficult to locate. There is no central recording of existing THS sites and not all THS addresses are published.

Where the Darknet really becomes black: While a large portion of Tor users are conducting legitimate business, anonymity on the dark side does lead to an increased potential for criminal activities. These activities include criminal marketplaces for drugs, child pornography, terrorism and other nefarious activities. The most prominent hidden marketplace on Tor was Silk Road.

The site enabled users to buy and sell illegal drugs and commodities. Silk Road was active from February 2011 until July 2013, where the site processed over $1.2 billion worth of illegal sales between 4,000 vendors and over 1,50,000 customers. The US Federal Bureau of Investigation took down the site in October 2013, although several other illegal sites have since taken its place.

Can we/should we block access to these sites? The long-standing public debate concerning online anonymity centres around the rights of individual citizens to be anonymous online, thereby protecting their freedom of speech and other individual freedoms or whether total anonymity leads to unethical and criminal behaviour.

Most governments agree that banning online anonymity systems completely is not an acceptable solution. China attempted to do so, only to discover that dissidents were using secret entrance nodes to the Tor network called “bridges” to continue their activities. Is the Internet our modern Silk Road?

THE FUTURE OF LEARNING: HACK-A-THONS AND CYBER LEARNING

S S Iyengar & Jerry Miller, Dec 31, 2015:

While no one can clearly define cyber learning, everyone seems to agree they are using it and point to its potential for transforming traditional modes of education to provide students a deeper, richer and more rewarding learning experience than would otherwise be possible. But what really is "cyber learning?" Is it working? And what does the future hold for this innovation?

Cyber learning has been defined as, "the use of network computing and computer technology to support learning." Perhaps, it can best be defined as the use of computer technology-assisted learning systems employed in teaching and learning which provide deeper inquiry experiences, creative problem-solving activities and intensive collaboration with other students.

Cyber learning allows us to explore new ways of understanding information while providing teachers with a more varied pathway to interact with and stimulate students through their combined, natural learning processes.

Cyber learning has been called by many names over the past few years, depending upon the adaptation of the computer technology for the learning objectives. It is expanding at an ever increasing rate. With the growth in delivery systems and our ability to adapt these systems as novel opportunities present themselves, we now have overlapping concepts and phrases to describe cyber learning, such as distance learning, blended learning, technology-assisted learning, traditional classroom instruction (which is incorporating computer technology more and more in its delivery), hybrid learning, online learning, mobile learning or "m-learning," and electronic learning or "e-learning," in addition to cyber learning.

Is cyber learning working? Before we can definitively answer this question, we must understand some of the unique challenges of cyber learning. We have already addressed one of the largest challenges, which is attempting to define cyber learning by constraining the definition to a specific delivery system. Today, we are combining many of these technology-assisted learning systems and applying them in unique ways, which make it difficult to assess the overall impact of a specific learning technology.

Another challenge we face is, understanding the learning styles or methods, and the learning process. While there are three main cognitive learning styles; visual, auditory, and kinaesthetic, there is a vast array of active

and traditional passive learning methods for which technology has been adapted. These include teaching others as we learn ourselves, practice by doing, discussion, demonstration, audio-visual, reading and lecture. Our retention rates decrease from approximately 90 per cent retention when we teach others to less than 5 per cent if we learn by listening to lectures.

While cyber learning technologies have been applied to each of these learning methods in order to increase the retention rate, it is difficult to say how effective specific cyber learning has been, since these technologies have been "blended" to improve overall retention rates.

What is the future of cyber learning? Recent studies, such as those presented in The International Journal of Information and Education Technology in August 2015, indicate that cyber learning is generally, "well accepted by the students as a supplement to traditional methods of teaching." Cyber learning has made an effective contribution to the improvement of learning outcomes, and will continue to do so well into the future.

In many cases, cyber learning allows participants to choose the place and time of their education, thereby enabling them to control their environments, receive the information when they are best able to learn and to ultimately, receive and retain more information at a faster rate. Students are also developing study sessions which incorporate cyber learning.

Hack-a-thons

Today, students worldwide are participating in "hack-a-thons." Unlike what you may think from the name, these are not events where subversive students meet to conduct cyber-attacks on government facilities, rather these events provide opportunities for large groups of people to engage in collaborative computer programming. These events can last from one day to an entire week, and provide the opportunity for computer programmers, graphic designers, interface designers, project managers and hardware development engineers to intensively collaborate on software and design projects.

Hack-a-thons also provide the opportunity for those engaged in these activities to learn by doing, as well as teach others skills that they have recently acquired, all within the realm of ever-expanding technology systems. In many cases, these hack-a-thons enable participants to build applications for learning which can be incorporated into online courses, within the classroom and learning through the use of mobile phones and tablets (m-learning). Cyber learning has expanded beyond the traditional classrooms and into business and industry.

One of the most successful emerging technologies is the use of virtual reality technology for training. Virtual reality allows us to develop 3-D representations of our environments, which technologists have adapted to enable learners to "see" inside engines as they are learning to make adjustments, to identify safety factors on the jobsite such as those encountered in the construction of skyscrapers, and to facilitate learning in a variety of other industries. In addition to improving employee learning, they are also reducing training and resource costs and improving safety.

It's not just the young who benefit from cyber learning. One of the most interesting uses of cyber learning technologies can be found on luminosity.com, a website which provides a series of games and tools developed

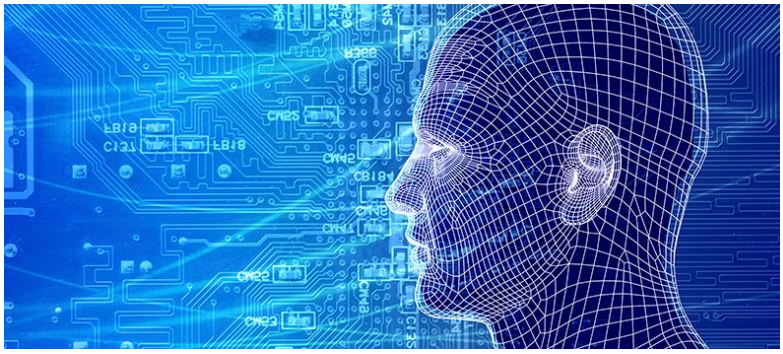
by a team of neuroscientists to provide personalised training targeting a wide variety of cognitive skills. Published results of the effectiveness of Luminosity's brain training have been mixed due to the complexity of variables surrounding brain science.

But, 70 million users in 180 countries seem to be enjoying the technology! Yes, cyber learning is here to stay. It will continue transforming our learning systems by incorporating rapid, efficient and effective computer-based learning technologies for use by young and old, as we rush to embrace the Knowledge Age.

DH
DECCAN HERALD
Archives
Like 482k
Google™ Custom Search
Search
Weather
Max: 28.8°C
Min : 18.8°C
In Bengaluru
Sunny day
Home | News | New Delhi | Business | Supplements | Sports | Entertainment | Videos | Opinion | ePaper |

BIOMETRICS AND DIGITAL FORENSICS: CYBER SECURITY CONNECTIONS

S S Iyengar and Jerry Miller, Dec 3, 2015



Most of us are familiar with biometrics, which is the use of fingerprints and other biologically derived data to specifically identify us as the unique people we are. We use biometrics to identify criminals, or to exonerate those falsely accused.

Traditionally, we have relied upon the unique pattern of fingerprints. As technology has advanced, we have been able to use other biometrics for identification.

Today, many advanced security systems rely on a retinal scan to identify patterns of veins in the back of the eye that also provide a unique identification pattern. Iris recognition has also become a popular identification means relying on the individual patterns and features found within the iris itself to provide a unique signature.

As the use of technology increases, so too does crime and terrorism. However, the increased use of technology also provides us an opportunity to derive new biometric and digital signatures to pursue those who engage in criminal and terrorist activities, as each electronic device has its own unique digital signature. Human interaction with our digital world also provides us with some interesting new digital biometrics.

Facial recognition has been one of the earliest and most popularly studied computer biometric applications and has remained so over the past 50 years.

While the initial attempts to explore facial recognition were made in the 1960s, it wasn't until Sirovich and Kirby developed the methodology for facial recognition in 1987, and Mathew Turk and Alex Pentland implemented the “eigenfaces algorithm” in 1981 that we could successfully use this method of identification.

Each of our faces is common in many respects but also unique in particular aspects, even among identical twins. If we can identify those general values, we can focus on facial scans for facial recognition, which rely upon the use of “eigenfaces” or local feature analysis to compose an a image.

“Eigenface” is a term derived from “eigenvalues” and “eigenvectors,” which exist in pairs and refer to the “vectors” or directions of values that provide the largest “variance” or difference in a set of data points.

By employing a process known as principal component analysis to a large group of human face images, we can generate a set of generalised eigenfaces.

These eigenfaces represent a set of standardised facial features, which can be combined in various ways to generate an approximation of specific individual faces. Since these eigenfaces are stored as a list of general values, rather than specific pixels of a digital photograph, storage space is significantly reduced.

The way we move and interact with our electronic devices also provides a unique form of identification. Studies have shown that the way we swipe our smartphones or the amounts of pressure we apply to computer and tablet keypads all are specific to us and provide a unique way of identifying exactly who is using a device. Even the way we carry and hold our devices provide interesting clues as to the identity of the users.

Digital forensics is an expanding branch of forensic science and it involves recovery and investigation of material found in devices in relation to cyber or other crimes. As more research is conducted, and as technology becomes more available and affordable so too will the methods of digital forensics expand.

Our computers, mobile phones, tablets, personal digital assistants (PDA), compact disks, digital camera flash cards and flash drives, and every electronic device capable of information storage can be a source of digital evidence.

This digital evidence is now used to prosecute all types of crimes, not just cyber or electronic crimes (e-crimes). A suspect's e-mail or mobile phone files could potentially contain critical evidence regarding the suspect's intent to commit a crime, their whereabouts during the crime, or their relationships to the victims.

The United States' National Institute of Justice (NIJ) and the National Institute of Standards and Technology (NIST) provide the National Software Reference Library (NSRL) to promote efficient and effective use of computer technology in the investigation of crimes involving computers.

This programme collects software from various sources and incorporates file profiles computed from the software into a Reference Data Set (RDS) of information.

Matching file profiles

Law enforcement, government and industry organisations can then use the RDS to review files on a computer by matching file profiles with digital signatures of known, traceable software applications.

Within the application, hash values in the hash set are applications which may be considered malicious, including steganography tools and hacking scripts.

Digital steganography is a method of concealing files, messages, images or video within another file, message, image or video. We are probably most familiar with steganography in the form of invisible inks used to hide messages between visible lines of and open or private letter.

The obvious advantage of steganography is that an intended, secret message does not attract attention, and can be openly transmitted, then decoded by the receiver.

Digital forensics can also help us unravel crimes involving document forgeries and counterfeiting which can be a direct accessory to criminal and terrorist acts. We are all familiar with the different techniques used to identify authentic bank notes, such as paper watermarks, security fibres, holograms, or special inks.

However, these security techniques can be cost prohibitive. Methodologies are currently under development to enable forensics experts to identify a variety of specific inks used in forging documents, as well as identify the "digital signatures" of the printing devices themselves.

As the future "Internet of Things" expands and connects us through the use of embedded computer chips with a multitude of mechanical devices, the use of biometrics and digital forensics will become an even more important element in our fight against criminal and terrorist activities.

DH
DECCAN HERALD
Archives
Like 482k
Google™ Custom Search
Search
Weather
Max: 28.8°C
Min : 18.8°C
In Bengaluru
Sunny day
Home | News | New Delhi | Business | Supplements | Sports | Entertainment | Videos | Opinion | ePaper |

CLOUD COMPUTING GOOD, BUT IT CAN BE DICEY TOO

S S Iyengar and Jerry Miller, November 5, 2015

Everyone seems to love the word "cloud," and why not? Technical benefits of the cloud abound. Cloud computing can, if used properly, reduce your operating costs and provide more security for your information. However, it can also be a recipe for disaster if you have not considered your business information needs and information access requirements.

"Cloud computing" means simply storing and accessing your data and programmes over the Internet, rather than on your computer's hard drive. Software is managed and upgraded off-site by a third party, relieving you of the responsibility of having your IT team manage data, associated hardware and security challenges. Cloud computing can be accomplished using "private clouds" as well as "public clouds."

Here are some cloud security concerns.

Many businesses have already made the switch to cloud computing. For those that have, congratulations! But was it the right decision? For those that haven't, maybe you should, but the perceived risks are holding you back. Or, perhaps you are one of a large group of business professionals who don't yet understand cloud computing and haven't made an informed decision.

Private clouds contain only your information and software while public clouds are provided as a service to a variety of users and have everyone's information stored on their servers. Both types use a third-party service provider and are built upon data centres, but are not the same as data centres. At this point, it is essential to differentiate between data centres and cloud computing.

In a typical data centre, information is stored either on-premise or in close proximity to the business. It requires hardware, software and personnel to manage the organisation and information flow. Access to data could be through a direct connection to the data centre, or with reach-back through the Internet to the one or two locations storing and maintaining data. Cloud computing is built across many data centres in multiple locations and offers reach-back access only through the Internet. Users typically share the costs for the service.

In a data centre, the business will likely have full control over their information. It is ideal for companies that need a customised, dedicated system that provides full control over their data and equipment. Since only the company will be using this infrastructure, a data centre is also more suitable for larger or specialised organisations that run many different types of applications and complex data workloads.

By design, a data centre has limited capacity – once the centre is built, you will not be able to significantly change the amount of storage and workload it can withstand without purchasing additional space and installing more equipment and software. Data security is also tied directly to the centre, its personnel and the access network connection.

However, cloud systems provide businesses with less actual control over their information although apparent virtual direct control is one of the cloud's selling points. Providers may state that you have "direct control" over your data, but it can only be accessed through the Internet.

If your link to the Internet service provider is severed due to power outage, equipment failure or, in some extreme cases, government control over Internet access, you will not be able to access your data unless you have it backed up on premise.

The three great advantages to cloud systems are lower costs, potentially improved security and scalability. In cloud computing, hardware costs are lower because all that is needed to access the system is an Internet connection and browser. Buying and constantly upgrading servers and other hardware may be unnecessary.

Many cloud providers claim they provide higher levels of security and uptime than a small or medium size business can typically provide on their own networks. As a result, the associated need for a large IT staff and continuous security software updates is diminished. If you need to expand data processing rapidly, cloud computing offers the best option, as a call to your service provider can quickly get you additional capacity.

Legal issues

Many providers, as well as their clients, argue that cloud computing provides the next generation of IT resourcing through a platform that is cheaper, scalable and more easily managed than local networks. Others argue that cloud computing is simply a form of outsourcing. There are, however, many legal issues raised by cloud computing.

At the heart of these issues is one cold, hard fact; cloud based IT management forces a business to entrust what is typically its most important asset – information – to a third party. Despite the many benefits of a cloud-based system, the loss of control over a company's information is probably the most significant psychological hurdle that cloud vendors (and clients) must overcome.

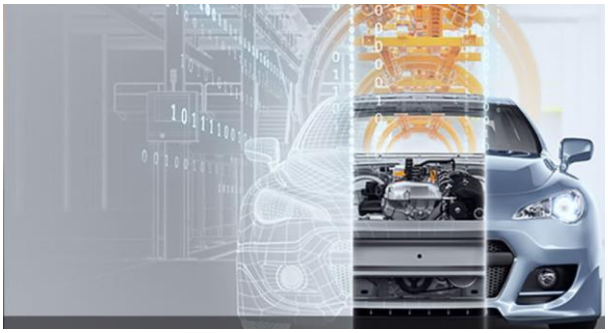
For most traditional businesses, when the computers shut down, so does the business. In today's modern businesses, however, 24 /7 operations can be essential. Having continuous access to your data may also be necessary. While widely advertised as giving the client 24/7 service, this may not always be the case. Your specific business model and data security/privacy needs for your industry must be considered before deciding if cloud computing is right for you.

Legal systems often lag behind adoption of technology. Contracts used by many cloud vendors essentially disclaim responsibility for data loss, downtime, or loss of revenue. In addition, governments have adopted statutory requirements applicable to many industries. Statutory and regulatory issues abound in healthcare, insurance and financial services industries. You, the business owner, are the only one who knows how security, privacy and access to your data relates to your business.

DH
DECCAN HERALD
Archives
Like 482k
Google™ Custom Search
Search
Weather
Max: 28.8°C
Min : 18.8°C
In Bengaluru
Sunny day
Home | News | New Delhi | Business | Supplements | Sports | Entertainment | Videos | Opinion | ePaper |

CYBER-PHYSICAL SYSTEMS WILL BE FUTURE DRIVER OF YOUR CAR

S S Iyengar and Jerry Miller, Oct 02, 2015, DHNS:



Do you know who's really driving your car, the bus, taxi, or train in which you're riding? For most of our older vehicles, the answer is obvious – the driver is in control. However, on newer model vehicles, almost all are operating with some form of embedded computer chip that is in control of vital elements, systems and processes within the vehicle.

These embedded systems are rapidly giving way to newer, more advanced systems known as cyber-physical systems (CPS). CPS are being incorporated into diverse product areas like aerospace, automotive, chemical processes, civil infrastructure, energy, healthcare, manufacturing, transportation, entertainment, and consumer appliances.

The CPS systems are engineered from, and depend upon, the seamless integration of computational algorithms and physical components working through a communications network that will transform the way people interact with engineered systems. This new revolution will provide endless new, creative capabilities for human-machine interaction, and has already spawned the "Internet of Things" (IoT) which will transform our interactions much like the Internet transformed our interaction with information. In the very near future computer systems will replace drivers in all of our vehicles. With the increased use of cyber-physical systems comes the increased threat of cyber security breaches.

Chrysler Corporation, America's third-largest automobile manufacturer recently announced a formal recall for 1.4 million vehicles which can be affected by a software vulnerability through the cars' "Uconnect®" dashboard computers. The Uconnect® dashboard computer integrates an 8.4 inch touchscreen on the vehicle's dashboard to enable access to navigation, integrated voice commands and Bluetooth, satellite radio and other entertainment systems as well as remote services that allow owners to start their vehicles and access vehicle systems and controls remotely.

Two security researchers, Charlie Miller and Chris Valasek, discovered and demonstrated this vulnerability in July 2015, when they wirelessly connected to a new Chrysler Jeep Cherokee, took over the dashboard functions, steering, and transmission, then disabled the brake system, causing the vehicle to go off the road and into a ditch – all from 16 km away. This was indeed, bad news for Chrysler, but good news for future cyber-physical systems.

Chrysler has already taken action to block the digital attack the researchers demonstrated by improving "network-level security measures" to prevent future penetrations. This involved additional security tools to detect and block these attacks emanating on a cellular carrier's network that allowed the vehicles to connect to the Internet.

The good news is that through the exploits of these researchers, CPS manufacturers will continue to develop cyber security measures to prevent attacks on their systems, or at least make them extremely difficult to hack. Even now, these attacks are not easy. Miller and Valasek worked for over a year to hack into the Chrysler system.

The software manipulation required a combination of unique and extensive technical knowledge, and prolonged physical access to the vehicles in order to break the code. However, in certain current and future cyber-physical systems, the opportunities for terrorists, criminals and enemies of the state to disrupt these systems may make the cost, time and effort worthwhile, all with devastating consequences.

The United States government's fiscal 2016 budget proposal requested $14 billion for cyber security efforts to better protect federal and private networks from hacking. Over $5.5 billion will go directly to the Pentagon to eliminate "significant vulnerabilities" in cyber networks, including weapons and weapon systems vulnerabilities.

In March 2015, US Defence Undersecretary Frank Kendall stated that cyber-attacks on US weapons, weapons programmes, and manufacturers were a "pervasive" problem to which the country must to pay a lot more attention. The United States is not alone.

India's Finance Minister, Arun Jaitley, has been criticised by the Centre for Strategic and International Studies, for having "not done enough… to make up the critical deficiencies in India's defence preparedness" in the 2015-2016 budget in order to meet growing threats and challenges. India's defence programmes have been quoted as being "…riddled with threats to cyber security," despite its well-known plans to spend approximately US $100 billion over the next 10 years on defence modernisation.

Vulnerabilities from CPS use

The United States and India, along with other nations, face similar threats and cyber vulnerabilities through the expanded use of CPS in national transportation and energy infrastructures. While future CPS technologies will enable capability, adaptability, scalability, resilience, safety, security, and usability that will far exceed the simple embedded systems of today, and improve innovation and competition in all sectors, vulnerabilities will be inherent in each of these new systems. Consequences of these vulnerabilities will be profound.

Traditional analysis tools are currently unable to cope with the full complexity of CPS or adequately predict system behaviour. For example, minor events that trip the electric power grid, which itself has evolved into an ad hoc network, can very quickly escalate into widespread power failures. Scientists and engineers must conceptualise and design for the deep interdependencies inherent between these engineered systems and the natural world.

Future challenges and opportunities for CPS will continue to be significant and far-reaching. With more autonomy and cooperation possible with CPS, greater assurances of safety, security, scalability, and reliability are demanded, placing a high premium on open interfaces and interoperability – areas which open us to cyber security vulnerabilities.

Two things remain certain. First, systems operating on our networks will always be vulnerable to attack and must be secured. Second, our future lives will be increasingly dependent upon cyber-physical systems, making us more vulnerable. A rational approach to the purchase and use of these items, as well as required standards of performance by business and industry to mitigate the threat will be essential. Caveat emptor!

DH
DECCAN HERALD
Archives
Like 482k
Google™ Custom Search
Search
Weather
Max: 28.8°C
Min : 18.8°C
In Bengaluru
Sunny day
Home | News | New Delhi | Business | Supplements | Sports | Entertainment | Videos | Opinion | ePaper |

BIG DATA AND CYBER SECURITY: WHAT HAVE YOU GIVEN AWAY?

S S Iyengar and Jerry Miller Sep 7, 2015,

Big data is a really big deal. Most of us are familiar with gigabytes (GB) and terabytes (TB) now that our flash drives and external hard drives are measured in these parameters. But do we really know how much data can be held on these devices?

If a person loads as many books as possible into a pickup truck and then stores them electronically, the data would consume only a 1 GB file. A 500 GB file could store all of the academic journal information currently contained on five library floors. Just ten 1-TB external hard drives could contain the entire printed collection of the largest library in the world, with more than 160 million items.

Today's digital information revolution has catapulted us from terabytes into petabytes (PB) and exabytes (EB) of information. With only 3 PB of storage space, we could contain all US and Indian academic research libraries, while 200 PB of information would contain the equivalent of all printed material on the face of the earth. If we were to capture all words ever spoken by human beings, we would have the equivalent of only 5 EB of information.

Beginning in 2000, the University of California, Berkley, conducted a study to estimate how much information is produced every year. They estimated that in 1999, the world produced between 1 and 2 exabytes of new, unique information.

By 2002, they estimated that 5 EB of new information in print, film, magnetic and optical storage media had been added. The study concluded that the amount of new information stored on paper, film, magnetic and optical media had almost doubled in the last three years, and grew 30 per cent each year between 1999 and 2002.

Today, our information flows through electronic channels – telephone, radio, television and the Internet – which contained almost 18 EB of new information in 2002, three and a half times more information than is recorded in storage media. Ninety-eight per cent of this total volume of traffic was information sent and received through telephone calls, land lines and wireless.

According to former Google CEO Eric Schmidt, every two days we create as much information as we did from the dawn of civilisation through the year 2003 – an astonishing five exabytes of data. Most of this data is user-generated content consisting of pictures, instant messages, tweets and posts.

It follows that the growth of digital information has led to exponential growth in the use of databases by everyone – individuals, governments, and businesses, as well as good guys and bad guys. "Big Data" has turned into "Big Business!"

What is big data? Big data is the term used to refer to collections of extremely large and/or complex databases that become difficult to process using conventional database management tools. These databases now contain on the order of exabytes of data. Data sets, such as those used for meteorology, Internet activity, or traffic flow where ubiquitous information sensors are constantly monitoring their environments and gathering data, are some of the reasons that databases have grown exponentially over the past few years.

Big databases are superior to smaller databases when used to evaluate detailed trend data, as additional, detailed information can be derived easily by looking across the expanse of data. This level of trend detail may be missed when relying on smaller databases – all good reasons to collect and use big data.

Downloading wirelessly

However, two items are especially troubling from a personal, as well as a national security perspective. Big databases enable everyone to collect more information about you – both government and commercial organisations. From an espionage standpoint, anyone can now carry 128 GB of information – more than 64 million pages of text – on a USB drive in their pocket and walk out of the door, having downloaded the data from any accessible computer. More disturbing is the fact that this data could have been downloaded wirelessly!

Information is being harvested through a variety of programmes by Internet Service Providers, local wireless providers, Internet browsers and other programmes. Data collection is a multi-billion dollar industry. By advancing big data collection efforts, companies now have access to tens of thousands of data sources on a specific individual that can be compiled within milliseconds. This information provides personal information to marketers, politicians and businesses to predict consumers' responses concerning healthcare, voter preference, and sales of everything from face creams to houses.

Google and other Internet and email providers mine your emails and searches for keywords in order to provide appropriate advertising. In many cases, companies don't need to mine data. We freely give birth dates, names, and other information in order to receive access or "free" services. Are these really "free" when the company is using your data to resell?

Cyber security and protecting your data: How can you protect your data? Since most of the information in the world today is being generated by you, are you controlling your information? Consider these things before your next social media experience turns into a cyber nightmare:

1) Think before you post! Know what data you are providing. Ensure you don't mind posting to the world. Remember, we provide most of the information ourselves which others can use to exploit us.

2) Know if it's "electronic data" someone can get access to it. Never disclose personal information by email. If you provide personal information on websites, use only official, secured websites of the company with which you are conducting business.

3) Never click on a security related pop-up on your computer. End the session immediately.

4) Install and run a security scan on your computer daily to prevent infections.

DH
DECCAN HERALD
Archives
Like 482k
Google™ Custom Search
Search
Weather
Max: 28.8°C
Min : 18.8°C
In Bengaluru
Sunny day
Home | News | New Delhi | Business | Supplements | Sports | Entertainment | Videos | Opinion | ePaper |

ROOTS OF MODERN 'CYBER' TERRORISM IN A DIVIDED WORLD

S S Iyengar and Jerry Miller, Agust 10, 2015

Global terrorism is an increasing threat. Previously framed primarily in terms of Al-Qaeda, today the landscape is swiftly changing. Terrorist groups are splintering into a blistering array of diverse actors with resiliency and adaptability – all exploiting social media and digital formats of the cyber realm for terrorist activities. Where did these threats originate?

In a world divided between us and them. The modern era of terrorism officially began with Al-Qaeda's declaration of war against the West in 1998. However, the roots of conflict run much deeper and are more widely dispersed.

"We are at the crossroads. We may join the march at the tail of the Western Caravan…or we may return to Islam and make it fully effective in the field of our own life," said Sayyid Qutb

Sayyid Qutb (1906-1966) was an Egyptian educator, member of the Education Ministry and the foremost Islamic thinker of his time. Qutb feared the Western powers' value of greed would crush the traditional Muslim way of life. He resigned from the Ministry of Education, shortly before joining the Muslim Brotherhood in 1953. An extremist organisation, the Brotherhood vowed to fight foreign influences and impose Islamic law "by the Koran and the sword." There, Qutb became one of the more outspoken figures as editor of the Brotherhood's newspaper, using print media to relentlessly publish withering criticisms of Egypt's pro-Western government.

Following a failed assassination attempt on President Gamal Abdel Nasser in 1954, Qutb was arrested, tried for his role in the event and imprisoned. Qutb's brutal, 10-year prison treatment, under some of the worst conditions in the world, began to inform his worldview, solidifying his ideas on the West and its influence on Islam.

While in prison, Qutb wrote a 30-volume study of Islamic scripture titled, 'In the Shade of the Qur'an', where he paralleled current world events to the time immediately prior to Angel Gabriel's revelations to Mohammed and the writing of the Quran. Known as the time of jahiliyyah – Arabic for "ignorance," or a state of barbaric chaos – it reflected the turbulent times of the late sixth century, when large portions of Arabia were occupied by foreign powers and warring tribes.

Only through intervention of Allah, his gift of the Quran, and establishment of Islam could followers bring order from chaos, subjugating a large portion of the world to Allah and sharia law. However, Qutb departed from traditional Islamic theology, advocating for two revolutionary concepts; offensive jihad and all-or-none Islam.

These two key radical interpretations were thus enthusiastically adopted by the more violent elements of Islam to circumvent the Qur'an's otherwise explicit prohibitions on killing, offensive wars and opposing existing Muslim leadership.

Qutb's cry for revolution was quickly taken up by members of the Muslim Brotherhood, some of whom had fled to other countries across the Middle East, including Qutb's brother Muhammad, who had escaped to Saudi Arabia where he would later mentor Osama bin Laden. Other followers remained in Egypt, including a young man known as Ayman al-Zawahiri.

In 1989, a perfect terrorist storm formed in a small meeting room in Afghanistan, where 10 Arab mujahideen, as well as Ayman al-Zawahiri and four other Egyptians, proposed establishing a new organisation called Al-Qaeda (the Base), in order to wage international jihad. These members represented an affiliation of individual mujahideen, established groups and the Egyptian Islamic Jihad rolled into one loose organisation funded by Osama bin Laden, and led by his right hand – operations expert Ayman al-Zawahiri.

The new group quickly established themselves with big plans and a hatred of all things Western. On September 11, 2001, their biggest plan came to fruition as they succeeded in destroying New York's World Trade Centre. Since that time, terrorist groups have splintered from this loose affiliation and taken up the mantel of modern terrorism using a variety of cyber methods to recruit members and wreak havoc.

Terrorist groups have expanded their base of operations, physically covering wide swaths across the Indian subcontinent, West Asia, and throughout Northern and sub-Saharan Africa. More importantly, their cyber presence is global.

Social media recruiting

One of the growing threats comes from the Islamic State of Iraq and the Levant (ISIL) who use advanced social media and Internet recruiting to increasingly fill their ranks with terrorist fighters. They use social media to inform, persuade and radicalise new individuals, as well as strengthen morale, reduce dissent and legitimise their use of terror.

Al-Qaeda in the Arabian Peninsula (AQAP) recently introduced Inspire Magazine, an English language online magazine filled with terrorist recruitment propaganda, improvised recipes for car bombs, and the bottom line message of Al Qaeda, "He who terrorises the enemy of Allah complies with the divine order... Inflicting terror on the enemies of Allah moves you closer to Him." First appearing in July 2010, the magazine recruits British and American readers to conduct domestic terror attacks.

In 2011, the Syrian Electronic Army (SEA) began using computer hacking as a means of waging war. The group, which supports Syrian President Bashar al-Assad, has since attacked and gained control of the

Associated Press Twitter account and had tweeted, “Breaking: Two Explosions in the White House and Barack Obama is injured,” setting Wall Street and world markets in a panic. They are continuously launching directed denial of service attacks, have gained control of websites and social media and defaced a variety of other sites.

Each day, new terrorist organisations enter the cyber realm to exploit the media, flame the passions of their supporters, and ruthlessly violate their victims. War is being waged relentlessly in cyberspace.

DH
DECCAN HERALD
Archives
Like 482k
Search
Weather
Max: 28.8°C
Min : 18.8°C
In Bengaluru
Sunny day
Home | News | New Delhi | Business | Supplements | Sports | Entertainment | Videos | Opinion | ePaper |

CYBER SECURITY: ARE SECRETS POSSIBLE ANYMORE?

By S S Iyengar and Jerry Miller, July 24, 2015

We hear a lot about cyber security these days, most of it bad. Cybercrime and associated cyber security breaches lead most of our technology coverage. Victims of these incidents may not even feel the ravages of the crime until it is far too late. They may already be economically dead, or at a minimum paralysed, with both their bank accounts and their identities gone before they even know they were victims of an attack. Perhaps, you are already one of its victims.

Consider for a minute some of these statistics. In 2014, cyber-attacks rose by 48 per cent, with over 42.8 million attacks occurring around the world. According to the Price Waterhouse Cooper Cyber Security Survey, security incidents cost businesses an average of US $2.7 million each year, with average reported losses up 34 per cent this past year. Perhaps, what is more important is that companies are identifying and reporting more incidents of higher monetary value.

Of those companies reporting losses greater than US $20 million this past year, the number of companies nearly doubled over reports from previous years! The fastest growing cyber threats involve attacks by peer competitors, organised crime, and even nation states, all of which increased by 86 per cent in 2014. And we are off to a banner year in 2015 already as evidenced by these accounts.

Anthem Healthcare Insurance was recently attacked with over 80 million personnel records compromised. Home Depot, a large US home improvement and hardware store, was also attacked and lost 56 million customer payment cards. More surprising was the cost to the company – over US $62 million – in order to take stop gap measures to secure the data, then inform clients of the breach and assure them Home Depot could be trusted to continue their business transactions.

And of course, who can forget the North Korean attack on Sony Pictures where digital records in several internal data centres were wiped clean, with sensitive contract information, salary lists, film budgets, social security numbers and even entire films stolen.

Experts believe that we may actually be engaged in a global cyber war where the lines between criminal activity and war can no longer be neatly drawn. According to a leading cyber security company, Kaspersky,

the top five countries most actively attacked are Russia, Germany, the United States, India and France, in that order.

Officials at the United States Government's Office of Personnel Management discovered after some time, that their files had been hacked, presumably by China, and "sensitive information" stolen. This information included the addresses and personal information, as well as health and financial information for over 4.1 million employees.

Later investigations revealed the attacks to have enabled the attackers to access not just 4.1 million records, but 14.1 million records. A short time later, it was revealed that the numbers were actually closer to 21.5 million records exposed with detailed information on the private lives of all US Federal employees over the past 15 years compromised, making this the largest cyber-attack and breach of information in US history.

How could so much information be compromised in these cyber security events? What is cyber security and what is this cyber domain we hear about? Will the prospects of compromised data grow even larger as we expand to cloud computing?

First, what is "cyber?" Cyber refers to anything relating to computers, information technology and/or virtual reality. The term "cyber domain" or "cyberspace" describes the environments in which we digitally live and work, and can be expanded to include anything in the electromagnetic spectrum, specifically as it applies to communications and information processing. All of communications media can be attacked and exploited.

For businesses, their clients demand more open access to the market, with expanded smartphone applications and opportunities for internet shopping from the comfort of their homes, 24 hours a day. Businesses have responded accordingly, expanding their shopping forums, as well as their exposure to cyber-attacks, yet their budgets for cyber security have actually gone down by 4 per cent over the last year.

Declining real security

But this is not an isolated statistic. Investment in cyber security by companies has remained steady over the past five years, resulting in rapidly declining real security. Simply put, companies are not keeping up with the cyber security threat.

So what is "cyber security" and how can companies better respond to the threat? Cyber security refers to actions taken to protect computer systems, networks, and information systems from disruption or unauthorised access, use, disclosure, modification, or destruction. There are three basic objectives of all cyber security measures – integrity, confidentiality, and availability.

First and foremost, the data in our systems must be protected to ensure that it is not tampered with either accidentally, or maliciously. This includes integrity of the data source, meaning that third parties do not have access to, nor responsibilities for, handling the information. The data, therefore, must be intact just as it was received from the source.

Information must also be accessible only to those authorised, thus ensuring confidentiality. This involves a series of protocols whereby access of information is restricted to those on access control lists, where their

"need-to-know" the information has been previously confirmed. Companies must ensure that access can only be made through proper hardware/software and only by those authorised.

Finally, companies must ensure that while their protective measures are in place, the data is actually usable, and can be accessed reliably in "real time." Information must be available immediately when needed, again without handling by third parties, or without providing too much information, and thereby exceeding the user's "need to know."