CONTENTS

PursuIT

MAY 2018 ISSUE

About the Journal

The e-Journal namely "PursuIT" is a platform for sharing of experiences and inculcate professional excellence in the field of IT Audit. The journal will have feature on the emerging areas of Information Technology viz. cybersecurity, Internet of Things, Artificial Intelligence. The journal will also look into the technological developments, future of technology, national policies and standards, as well as articles on IT Audit conducted in various SAI's.

Editorial Board

Online Submission of Articles

To support this initiative of e-journal, we welcome you to contribute Electronic submission of articles from the fields of IT audit and Emerging areas in the IT field. The article should be relevant to the theme and should be of minimum 1000 words. All submissions should be accompanied by a short profile of the author. The articles may be forwarded to icisa@cag.gov.in.

Feedback/Suggestions

We strive for constant improvement and encourage our readers to provide their valuable feedback/suggestions to make the endeavour successful. Send us your suggestions, comments, and questions about the e journal to icisa@cag.gov.in.

Disclaimer

Facts and opinions in articles of the journal are solely the personal statements of respective authors and they do not in any way represent the official position of Indian Audit and Accounts Department. This Journal is for internal circulation within Indian Audit and Accounts Department only. The contents of this journal are meant for informational purposes only. iCISA disclaims all liability for actions taken or failed to be taken based on any content of this journal.

From the desk of Director General, iCISA

e – Governance initiatives of GOI have resulted in creation of new systems and modes of delivery of goods and services resulting in paradigm shift in the manner in which work is done. This evolving eco system has resulted in its own share of risks and threats. It has also been noticed that there is an increased dependence of the common people on IT applications while at the same time their awareness about the risks associated with new modes of delivery needs to be updated.

In this changed scenario it has become necessary to disseminate the knowledge about the new developments and the manner in which the people will be impacted by new technologies. Since its formation in 2002, iCISA has contributed to the world audit fraternity through its training programs. In the past there has been a practice of sharing the latest developments in the Information Technology matters by way of an Online Journal PursuIT. We have decided to start this practice again on a bi-annual basis and the first Journal in this series is being issued with the theme of "Emerging Threats, Risks and Vulnerabilities in the Cyber world".

I am sure that it will of immense value to the readers. A lot of effort has gone into bringing it in its present form and the efforts of the officers who have contributed to it needs to be appreciated. We will need invaluable suggestions of the readers to make it even better in days to come.

Ram Mohan Johri
Director General
iCISA

Theme article

Digi-Trends, Technologies and Risks

Compiled by: Ramadevi Lakshmanan, SWIFT, Malaysia

Profile of Author

Ms. Ramadevi Lakshmanan is an Agile Strategy Lead/Enterprise Agile coach in SWIFT, Kuala Lumpur, Malaysia. She has over 20 years of IT experience including 8 years of Agile experience in Scrum, XP, Kanban, DevOps and SAFe; and 12 years of Client delivery management, project management and software development experience in Communications, Financial Services, Healthcare, Manufacturing and Retail domains on multiple technologies such as JAVA, .NET, Oracle Applications ERP, Siebel CRM etc. Her professional certifications include, CSM, TKP, SAFe Agilist and ITIL.

This age of Innovation, no doubt, brings new trends and technologies on a daily basis to our desks (computers, smart phones, wearables etc.). Though the 'upto the minute' trends are taking 'Generation Z' to the hi-fi life style of ease of use, saving of time and costs, yet social websites and integrated internet services are posing big questions against the privacy and data security concerns. This article intends to outline the recent promising digi-trends, namely Internet of Things (IoT), Blockchain technology and Artificial Intelligence, which however come packaged with heavy risks. I intend to describe the feasibilities on how to handle these risks, too.

Technology and Risks

Technology, being a sharp knife, brings new opportunities and threats equally. Mankind, with its everlasting zeal, would deal with these emerging risks with mitigation strategies and innovative solutions. The solutions themselves, sometimes lead to new risks, resulting in this vicious cycle of innovation-risk-mitigation and innovation.

Thus, it goes without saying that any innovation should be embraced along with the associated risk assessment and mitigation plans. The organisations adopting the innovation need to follow 'Inspection and Adaptation' principle to spot for the risks continuously, assess the risks on an ongoing basis, arrest the impacts instantly and adapt the mitigation solution at all times.

Integrated iServices and IoT:

Technology has made it possible for everyone to live the life of a king. When trillions of devices, networks and services are connected together they replace those 'n' number of servants in your palace.

Imagine the royal life of your alarm waking you up and also simultaneously sending a signal to the coffee brewing machine, and the coffee is served as you get up from the bed. (Sooner, a Virtual Assistant may bring it to your bed too!). As you drink the coffee, the attached sensor sends a signal to switch on the Geyser and stops at the right temperature based on the historical bath data of yours. You come out of home now and the driverless car comes to the entrance and takes you to the office by the route with least traffic. This phenomenon is what, in technological terms, called as 'Internet of Things', or simply IoT.

Another interesting feature here is that some of these 'things' are on your body too – called as Wearables. Take your fitness tracker, - some small application sitting inside that wearable, knows more details about you than your family doctor. The Google glass wearers are able to communicate in natural language. The world of convenience enabled with IoT definitely leads to personal safety and security concerns as well.

When Google reminded us about the upcoming flight, we do feel royal, having such an efficient personal assistant. However, on a deeper thought, one does realise that our e-mails are read by this assistant to convey us the information about our flight schedule. It means

the privacy of my mail communications gets compromised. Yet, we are helpless as we don't seem to stand a chance of a life in exclusion of such technologies, henceforth.

Even if any one of the 'things' in this IoT network is hacked, it will lead to information leakage from all the devices connected to. What if one's car is hacked by a business rival. It may drive you to hit an accident. Now, the royal life seems to have equally royal dangers and threats related to security, privacy and data sharing. And, technically speaking, along with it comes the challenge of infrastructure. Say, for example, the amount of data the whole IoT produces is huge and it will be a challenge to store and maintain the same.

Now, the same world of convenience enabled with wearables definitely puts the safety of your person and information at risk, more than ever.

Yes, the industry has started listing the potential impacts the technology come carrying. A regulatory body to standardise the norms may help to reduce the risks but not completely avoid the same. So the risk sustains till the industry experts figure out better ways of handing IoT in a more secured way.

Blockchain and BI:

"The blockchain is an incorruptible digital ledger of economic transactions that can be programmed to record not just financial transactions but virtually everything of value." - Don & Alex Tapscott, authors Blockchain Revolution (2016).

William Mougayar, Venture advisor, 4x entrepreneur, marketer, strategist and blockchain specialist, explains Block chain technology with the 'Google Docs' analogy. He says, "The traditional way of sharing documents with collaboration is to send a Microsoft Word document to another recipient, and ask them to make revisions to it. The problem with that scenario is that you need to wait until receiving a return copy before you can see or make other changes because you are locked out of editing it until the other person is done with it. That's how databases work today. Two owners can't be messing with the same record at once. That's how banks maintain money balances and transfers; they briefly lock access (or decrease the balance) while they make a transfer, then update the other side, then re-open access (or update again).With Google Docs (or Google Sheets), both parties have access to the same document at the same time, and the single version of that document is always visible to both of them. It is like a shared ledger, but it is a shared document. The distributed part comes into play when sharing involves a number of people.

Imagine the number of legal documents that should be used that way. Instead of passing them to each other, losing track of versions, and not being in sync with the other version, why can't "all" business documents become shared instead of transferred back and forth? So many types of legal contracts would be ideal for that kind of workflow. You don't need a blockchain to share documents, but the shared documents analogy is a powerful one."

Blockchain, being highly decentralised data network based on digital currencies to ease financial ledgers process and transactions, the idea is to maintain data integrity and availability. This enables Data Analytics and Business Intelligence (BI), to leverage this decentralised data storage and management for the growing needs of data and decision making sciences. Apart from this, Blockchain promises the business users the ability to create value and authenticate digital information through many new business applications like Smart Contracts, Supply Chain Marketing, Crowd Funding etc.,

Though the Blockchain architecture, is supposed to be invincible, in practice, in theory, Cyber security is a serious threat. Secured coding and data setup to prevent the vulnerabilities would help. Tight security controls should be in place to avoid security breaches.

The way of life is, if the cops are smart, thieves are smarter. It has become the need of the day that the people who innovate technologies should demonstrate smartness of the hackers in their

inventions and make them hack-proof. The organisations also need resources with protector mindset operating 24/7. That is where the security compliance and practices put forward would help with.

Automation and AI:

Artificial intelligence (AI) is a term for simulated intelligence in machines. These machines are programmed to "think" like a human and mimic the way a person acts. The ideal characteristic of artificial intelligence is its ability to rationalize and take actions that have the best chance of achieving a specific goal, although the term can be applied to any machine that exhibits traits associated with a human mind, such as learning and solving problems.

"AI is changing the way in which organisations innovate and communicate their processes, products and services, AI continues to drive change in how businesses and governments interact with customers and constituents." says Whit Andrews, research vice president and distinguished analyst, Gartner.

Artificial Intelligence breaks the human limitation barriers, thus playing a very productive role. However, the risks are also enormous. Say for example, in Health care, if the data is not adequate, an AI decision may lead to disaster and play havoc with human lives. The best way to deal with this is to couple human thinking with machine analysis, as a control mechanism, at least, in the short run. As neural network emerges with new inputs, there is a need for us to establish the new connectivity with the exiting AI solutions.

Though AI is progressing, the path is very bumpy. Conversational AI and Emotional AI are some of the exciting inventions though, in its nascent stages. AI is leading to other dynamics like its impact on the job market. Some IT services company have already started lay off in the name of automation and AI, threatening a number of jobs. Nothing can stop a technology, whose time has come. Instead of workforce reduction, organisations may consider diverting the same into risk management, continuous improvements and innovations to address the emerging risks.

Now what?

The above mentioned digi-trends called IoT, AI and Blockchain are capable of and are transforming business models and user experience like never before. They have enormous potential to enhance the underlying economics of specific business processes, to drive higher productivity, make work and domestic environment more efficient and deliver value. In addition to boosting productivity, the technologies are also making a difference to quality and cost, in both personal and official fronts. Yet, they come with great risks to valued attributes of life like Privacy, Personal safety and Security. Apart from regulatory mechanisms in the governance of these technologies, the industry also needs to gear up in the management of risks. The IT organizations and its customers are already into lot of rework due to software upgrades, OS patches, hardware advancements etc., The way software products are developed and delivered also keeps evolving since the introduction of Agile 2001.

"If we continue to develop our technology without wisdom or prudence, our servant may prove to be our executioner" said, Omar Bradley (General, US Army). It is a period of transition and transformation and I am sure, that mankind will pass through this stage; and using the same strength with which it had conquered epidemics and pandemics in the previous centuries, conquer the various risks associated with these digi-trends and use them for the betterment of the human race.

Reference :

1. https://www.forbes.com/sites/robertbtucker/2018/01/29/eight-technology-trends-ready-for-exploitation-in-2018/2/#5b3c374a4a43
2. https://www.gartner.com/smarterwithgartner/gartner-top-10-strategic-technology-trends-for-2018/
3. https://www.gartner.com/technology/books/digital-disruption/
4. https://chapters.theiia.org/san-diego/Documents/Seminars/SD_IIA___ISACA_Event_041112_Deloitte_IA_Top_Ten_Risks.pdf
5. https://www.smartinsights.com/digital-marketing-strategy/wearables-statistics-2017/
6. https://blockgeeks.com/guides/what-is-blockchain-technology/
7. https://www.investopedia.com/terms/a/artificial-intelligence-ai.asp#ixzz5EPc3OWu3

IT Audit Highlights: Various Supreme Audit Institutions

Investigation report on the WannaCry Ransomware attack by National Audit Office, United Kingdom

The WannaCry ransomware attack (May 2017) was a worldwide cyber attack by the WannaCry ransomware cryptoworm, which targeted computers running the Microsoft Windows operating system by encrypting data and demanding ransom payments in the Bitcoin cryptocurrency. It propagated through Eternal Blue, an exploit in older Windows systems released by 'The Shadow Brokers' a few months prior to the attack. While Microsoft had released patches previously to close the exploit, much of WannaCry's spread was from organizations that had not applied these, or were using older Windows systems that were past their end-of-life. WannaCry also took advantage of installing backdoors onto infected systems.

National Audit Office (NAO) UK investigated the National Health Services (NHS) response to the cyber-attack that affected it in May 2017 and the impact on health services and a report to that effect was published (Oct 2017). The highlights of the investigation report are presented below and the full report can be read at:

https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf

WannaCry was the largest cyber-attack to affect the NHS in England, although individual trusts had been attacked before 12th May 2017. The investigation focused on the ransomware attack's impact on the National Health Services and its patients; why some parts of the NHS were affected; and how the department and NHS national bodies responded to the attack.

The department was warned about the risks of cyber-attacks on the NHS a year before WannaCry. The attack led to disruption in at least 34% of trusts in England although the department and NHS England did not know the full extent of the disruption.

Thousands of appointments and operations were cancelled and in five areas, patients had to travel further to accident and emergency departments.

The Department, NHS England and the National Crime Agency informed the NAO that no NHS organization paid the ransom, but the department does not know how much the disruption to services cost the NHS. The cyber-attack could have caused more disruption if it had not been stopped by a cyber researcher activating a 'kill switch' so that WannaCry stopped locking devices.

The Department had developed a plan, which included roles and responsibilities of national and local organizations for responding to an attack, but had not tested the plan at a local level.

NHS Digital informed NAO that all organizations infected by WannaCry shared the same vulnerability and could have taken relatively simple action to protect themselves. Infected organizations had unpatched, or unsupported Windows operating systems so were susceptible to the ransomware. The NHS has accepted that there are lessons to learn from WannaCry and is taking action.

https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf

Cyber security: Follow-up Audit by Australian National Audit Office

In 2014, the Australian National Audit Office brought out a report named, 'Cyber Attacks: Securing Agencies' ICT Systems'. The crux of the report is presented below and the full report could be accessed at https://www.anao.gov.au/work/performance-audit/cyber-attacks-securing-agencies-ict-systems

ANAO examined seven Australian Government entities' implementation of the top four mandatory mitigation strategies in the Australian Government Information Security Manual, that is, application whitelisting, patching applications, patching operating systems and minimising administrative privileges.

Audit noticed that none of the seven entities were compliant with the Top Four mitigation strategies. Audit also examined entities' cyber resilience, which includes establishing a sound ICT general controls framework and effectively implementing the Top Four mitigation strategies; and the ANAO adopted the high level assessment criteria to assess the same.

In 2017, the ANAO conducted a follow-up audit, revisiting three of the original seven entities. This report can be accessed at https://www.anao.gov.au/work/performance-audit/cybersecurity-follow-audit. The ANAO assessed that of the three entities only the Department of Human Services was compliant with the Top Four mitigation strategies. The Department of Human Services also accurately self-assessed compliance against the Top Four mitigation strategies and met its commitment to the Joint Committee of Public Accounts and Audit of achieving compliance during 2016.Cyber resilience is the ability to continue providing services while deterring and responding to cyber-attacks. Cyber resilience also reduces the likelihood of successful cyber-attacks.

https://www.anao.gov.au/work/corporate/commonwealth-auditors-general-group-e-newsletter-issue-1-april-2018

Know more interesting features on 'cyber Security' here

1. Facts about Cyber crime - https://www.youtube.com/ watch?v= PIELVMQhvXc
2. The 15 worst data security breaches of the 21st century - https://www.youtube.com/watch?v=Kik9xgZcf9I
3. Top 10 Data Breaches - Biggest Hacks - https://www.youtube.com/watch?v=96VDo2yv3-g

Supreme Audit Institution- INDIA

1. Workflow Automation in Government of Odisha: Report on IT initiative in the State of Odisha by SAI India

Government of Odisha implemented a workflow automation system, i.e. Odisha Secretariat Workflow Automation System (OSWAS) at the State Secretariat. OSWAS aimed to achieve efficiency and effectiveness in its functioning. Information Technology Audit of OSWAS exposed deficiencies in IT Governance, Controls and Security leading to system being unreliable.

Various deficiencies noticed in course of audit are summarised as under.

Even after six years of implementation, all envisaged core, common and Department specific applications could not be developed. All key features and deliverables as per Service Level Agreement (SLA) viz. biometric access control, secure server layer (SSL), email/fax integration and source code delivery could not be ensured.

Odisha Computer Application Centre (OCAC), the nodal agency for implementation of OSWAS could not exercise adequate control over database administration activities nor segregated the key administration job or placed compensating controls.

Access controls:
Access controls were found inadequate in OSWAS as the files were accessible to any user irrespective of department, post and confidentiality.

Input and validation controls:
Due to absence of controls, the timestamp on notes in files at more than one level were exactly same. Similarly, it was noticed that in 679 files and 6764 documents, single user created notes at exactly same time.

OSWAS did not ensure accountability as database analysis revealed 31027 notes created in OSWAS did not depict names of notes creator/user as the records of such users were deleted at back end from user master.

Inefficient user management:
User management in OSWAS was inefficient as 400 active users were not available in LDAP server used for authentication. Besides, login names were reused leading to reduced level of accountability.User management was given to the vendor without any control of OCAC.

Implementation of digital signature in OSWAS for notes/documents was found non-compliant to IT ACT 2000 due to which non-repudiation could not be ensured.

Business Continuity and Disaster Recovery Plan was not framed.

Critical Government processes/functions were at a risk of disruption in the event of a disaster. Backups were inadequate and were never tested for restoration. The complete IT Audit report is available at the following link.

http://icisa.cag.gov.in/view/pdf/aHR0cDovL2ljaXNhLmNhZy5nb3YuaW4vYXVkaXRfcmVwb3J0LzI1LzU5YjBlZTEwMDVlNThlNmNmNzFmNjVkZWM1ZDQxNDUyLnBkZg==

2. IT audit on implementation of Financial Accounting Package in Food Corporation of India:

Food Corporation of India (FCI) rolled out FAP without the pilot locations expressing their satisfaction and full payment of ₹ 12.53 crore was released to TCS. You can read the full report at http://www.cag.gov.in/sites/default/files/audit_report_filesUnion_Commercial_Compliance_Report_15_2016_Vol.%20I.pdf. However, the summary of the report is given below:

Financial Statements could not be generated through FAP due to deficient customisation and these were being prepared manually.

Modules of FAP lacked proper validation, security provisions and processing controls leading to incorrect output, unreliable data and excess payments.

No log files depicting login details of users such as login date/time, IP address etc., were maintained in the system. There were instances where all the staff of Accounts section were found using the same user ID and password and thereby compromising the security of the system and also making it difficult to fix responsibility in case of any misuse.

The logic to calculate depreciation was incorrectly configured in the system in violation of the Companies Act 2013 whereby the application calculated depreciation on the full useful life of the asset rather than on remaining useful life of the asset.

Mandatory functions like calculation of Service tax rates, VAT rates, Standard rates etc. were not configured in the application and they continued to be calculated manually making them prone to human errors.

Theme article

Cyber Security and Connected Legalities – Emerging Risks in Information Technology

Compiled By Pavan Duggal
Advocate, Supreme Court of India, Chairman,
International Commission on Cyber Security Law President,
cyberlaws.net

Profile of Author

Pavan Duggal, is a practicing advocate in the Supreme Court of India at New Delhi and a consultant to UNCTAD and UNESCAP on Cyber law and Cybercrime respectively. He is the Founder President of Cyber law Asia, Asia's pioneering organization committed to the passing of dynamic cyber laws in Asia. He also has to his credit, the pioneering work in the field of Convergence Law

The world today increasingly is a connected world. Internet has made **geography history.** However, with connected networks which are forming a ubiquitous part of our day-to-day lives, it is increasingly getting important that security of computer systems and networks is becoming of crucial significance. No wonder, these days we are beginning to hear tremendous news about cyber security. In fact, over a short period of time, cyber security as a concept has tremendously increased in its scope, applicability and ambit. For the last few decades, everyone was talking about first, computer security and then, information security. The advent of the concept of cyber security has brought far bigger and ever expanding vistas & horizons within the ambit of the subject.

What exactly is cyber security?

Wikipedia has defined *Cyber Security or Information Security* as security applied to computing devices such as computers and smartphones, as well as to both private and public computer networks, including the whole Internet. The field includes all the processes and mechanisms by which digital equipment, information and services are protected from unintended or unauthorized access, change or destruction, and is of growing importance due to the increasing reliance of computer systems in most societies[1].

Cyber security is defined as the body of technologies, processes and practices, designed to protect networks, computers, programs and data from attack, damage or unauthorized access. In a computing context, the term security implies cyber security[2].

According to Merriam Webster Dictionary, cybersecurity[3] means measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack.

Cyber security, also referred to as information technology security, focuses on protecting computers, networks, programs and data from unintended or unauthorized access, change or destruction[4].

Cyber security is emerging as an important risk in Information Technology in general, and specifically, in the context of IT audit.

In the last few years, cyber security has assumed tremendous significance. The number of cyber security breaches are constantly growing with each passing day. As a result, the annual cost of cybercrime is constantly increasing. As per a recent survey, it has been estimated that the total global cost of cybercrimes is expected to cross USD 6 trillion by 2021. Hence, the protection and

preservation of cyber security becomes an important priority for all stakeholders.

The breaches of cyber security numbers will massively increase. When one looks at the statistics of cyber security, it tends to present a very frightening picture.

The estimated annual cost for cybercrime committed globally has added up to 100 billion dollars[5]. 9,740,567,988 data records have been lost or stolen since 2013. Everyday 5,153,740 records are stolen[6]. 95% of breached records came from three Government, retail, and technology industries in 2016[7]. In the past year, nearly 700 million people in 21 countries experienced some form of cyber-attack[8].

Since the year 2017, we have begun seeing massive increase in cyber security breaches. The year 2017 saw the Wannacry ransomware attack in more than 50 countries across the world. The cost of losses caused by Wannacry ransomware attack have not yet been calculated. We also saw Petya ransomware attacks and thereafter Equifax cyber security breach in the US, which woke up various stakeholders from their slumber.

The year 2018 began with a bang. The World Economic Forum (WEF) 2018 Global Risks Report includes cybersecurity threats as one of its four key areas. It predicts that cyber-attacks will constitute the third largest global threat in 2018[9]. The average cost of data breach in 2020 will exceed $150 million, as more business infrastructure gets connected[10].

Hence, all stakeholders who are dealing with any of the seven raw materials in the digital and mobile ecosystem i.e. computers, computer systems, computer networks, computer resources and communication devices as also data and information in the electronic form need to now be concerned with cyber security in a big manner. This assumes more significance, as nation states are beginning to wake up to the necessity to come up with legislative mechanisms and frameworks to deal with regulating different aspects of cyber security.

It needs to be understood that at an international level, there is no universally applicable international Cyberlaw in place which cover issues pertaining to cyber security. The only nearest example that comes up in this regard is the Budapest Convention and the Convention on Cybercrime of the Council of Europe which only deals with issues pertaining to regulating cybercrimes.

Further, since large number of Critical Information Infrastructure across the world is in private hands, it becomes the bounden duty and responsibility of private non-state actors to ensure the protection and preservation of cyber security.

Countries have begun to realize that given that there are no international Cyberlaw frameworks to deal with cyber security, they ought to increasingly engage in bilateral arrangements. Consequently, we have begun to see various countries coming up with bilateral cyber security cooperation mechanism and agreements. These would include various bilateral treaties between different nations including China-US, US-UK, India-US, India-UK, India-Malaysia etc. Most of these bilateral arrangements have been formed on the basic premise that countries need to collaborate with each other on bilateral basis to promote exchange of information pertaining to cyber security breaches and further countries need to take steps to not hack each others' critical information infrastructure and other related systems.

While the efficacy of bilateral arrangements in the field of maintaining global challenges of cyber security breaches is a questionable point but the fact still remains that these bilateral arrangements are a step forward in the right direction.

Meanwhile, countries have also begun legislating new cyber legal frameworks to deal with cyber security. The foremost country in this regard that still lead in cyber security law jurisprudence is China. China came up with its law on national security in July 2015. China's new law on national security including cyber security represents a new approach and methodology of dealing with the issue of cyber security. The legislation breaks new grounds inasmuch as it seeks to intermingle cyber security as an integral component of national security.

Thereafter in November 2016, China passed its first cyber security law, which came into effect on 1st June 2017. This law is known as The Cybersecurity Law of the People's Republic of China, which got implemented on 1st June, 2017. This law has provided for various compliance requirements for not just companies in China but also for companies out of China or targeting the Chinese market. In addition, China also included the elements of data localization. It also provided increasing liabilities and penalties for non-compliance with the parameters of Chinese law. Effective 1st January, 2018, China came up with a new Chinese law being Public Internet Cyber Security Threat Monitoring and Mitigation Measures. China has taken a lead in this direction, by coming up with its legal framework on cybersecurity. This approach could potentially encourage other nations to start thinking in the direction of regulating activities in the cyber security ecosystem for monitoring and mitigating Public Internet Cybersecurity Threats.

In addition, we have seen countries like Germany coming up with national legislations on cyber security. The German national law on cyber security has adopted a different approach and has focused more on critical information infrastructure.

Singapore has in February, 2017 passed a new cyber security law which aims to look at regulating at a holistic perspective, various issues, aspects and activities pertaining to protection and preservation of cyber security in the digital ecosystem.

We have begun to see different countries coming up with their own national policies on cyber security. These national policies constitute good motherly statements of the vision of respective nations on what they plan to do in the context of promoting and strengthening cyber security.

When one looks at the global map of emerging cyber legal developments concerning cyber security, it is increasingly getting clear that countries are beginning to come up with new compliance requirements, in the context of protection and preservation of cyber security. Hence, all stakeholders who are dealing with data and information in the electronic form, have to be intrinsically now prepared for a new set of compliances being mandated by the cyber security legislations in different parts of the world.

It needs to be noted that these compliances need not to be taken lightly as the non-compliance with the said mandatory compliances could expose the stakeholders to various kinds of legal consequences. They could be exposed to not just damages by way of compensation but also to criminal liability which could consist of imprisonment and fine. Hence, increasingly all stakeholders generally and specifically IT auditors in particular have to now be concerned with not just the significance of cyber security but also the need for proactively complying with the compliance requirements pertaining to emerging cyber security legislations.

When one looks at the global landscape, one feels that this kind of trend is only going to strengthen in terms of countries coming up with more legislative mechanisms to promote, strengthen and further substantiate cyber security protection and preservation.

As time passes by, it is increasingly getting very clear that cyber security will continue to keep on getting more importance. This becomes even more relevant, given the fact that emerging technologies are now attracting the attention of the world community to cyber security. With the advent of the Internet of Things, it is expected that 50 million devices will get connected to the Internet in the next couple of years, opening up a new vista of cyber security challenges.

Further, the advent of Blockchains and its various applications in different areas of human activities now increasingly focus upon the need for looking at cyber security in the context of Blockchain ecosystem. The advent of Artificial Intelligence has further now anticipated the need for new focus on interconnection between cyber security and Artificial Intelligence.

In this context, thus the IT audit ecosystem needs to be specifically aware of the new emerging technological developments and their impact on cyber security. The IT audit stakeholders need to

be aware of not just the significance of cyber security but also the need for proactively complying with various new compliance requirements that are being increasingly mandated by different national legislations in different parts of the world.

Compliance with these increasing legislative frameworks becomes important for not just escaping exposure to potential legal liability but also for the purposes of further strengthening the digital ecosystem in general.

Needless to say in the actual day-to-day working of the IT audit ecosystem, the international best practices pertaining to protection and preservation of cyber security will also have to increasingly be complied with, with utmost regularity and proactively.

It is expected that over a period of time, countries could also experiment with the concept of data localization so as to further ensure protection and preservation of cyber security. Though data localization as a paradigm may ultimately not be very conducive to the global paradigm of the Internet, yet countries are adopting different national approaches to come up with new mechanisms to deal with protection and preservation of cyber security.

As we look forward to further new developments taking place this year, it is increasingly clear that stakeholders in the digital ecosystem in general and the IT audit ecosystem in particular will need to definitely be taking cyber security as a significant vector and parameter for attention. Cyber security will now continue to govern day-to-day professional, personal and social lives in the next few years and decades. Hence, there is also a need for inculcating cyber security as a way of life as a culture as we go forward. This is a very rapidly developing field. Lot of new developments are constantly happening. Stakeholders in the IT audit ecosystem will have to be keeping their ears to the ground in order to find out not just the new developments in cyber security but also to come up with new, adequate and enabling approaches to deal with newly emerging challenges pertaining to cyber security.

Cyber security law is a fascinating area of newly emerging jurisprudence under the Cyberlaw umbrella. This area of jurisprudence is likely to massively evolve in the coming times. It will be really interesting to see how the digital ecosystem in general and the IT audit ecosystem in particular adapts itself to constantly evolving and newly emerging challenges and breaches concerning cyber security.

According to Cyber Security Hub, Grand View Research has predicted that spending on threat intelligence products and services will reach $12.6 billion by 2025. All signs point to an increase in cybersecurity spending and investment[11].

In conclusion, it can be stated that cyber security is the foundation for the digitally connected ubiquitous future. More nations and different stakeholders invest in cyber security not just as an emerging risk but also as an emerging opportunity. The better cyber security will serve the cause of not just individual, national, regional and international growth- the better it will help to ultimately make the Internet a far more robust ecosystem on which our everyday life is dependent.

It will be interesting to see the developments in this regard as we move forward.

[1] *https://en.wikipedia.org/wiki/Computer_security*

[2] *whatis.techtarget.com/definition/cybersecurity*

[3] *http://www.merriam-webster.com/dictionary/cybersecurity*

[4] *http://www.umuc.edu/cybersecurity/about/cybersecurity-basics.cfm*

[5] *https://www.cybintsolutions.com/cyber-security-facts-stats/*

[6] *http://breachlevelindex.com/*

[7] *https://www.cybintsolutions.com/cyber-security-facts-stats/*

[8] *https://www.comparitech.com/vpn/cybersecurity-cyber-crime-statistics-facts-trends/*

[9] *https://www.weforum.org/reports/the-global-risks-report-2018*

[10] *https://www.cybintsolutions.com/cyber-security-facts-stats/*

[11] *https://securityintelligence.com/news/ cybersecurity-spending-poised-to-rise-in-2018-gartner-reports/*

Audit Aids

Integrity Issues to be kept in Perspective During Audit of E-procurement Systems

Compiled by: Jitendra Kohli, Managing Director, ElectronicTender

Profile of Author

Mr. Jitendra Kohli is a Bachelor of Technology in Electrical Engineering from the Indian Institute of Technology, Delhi. He is the founder and Managing Director of ElectronicTender an e-Procurement technology lab.

He has been researching in the area of e-procurement/ e-tendering, with focus on public procurement, for over 18-years now. Based on his research, his company, ElectronicTender has developed a cutting-edge e-procurement/ e-tendering/ e-auction software product, Electronic-Tendering Engine (ETE) for public-procurement.

Background

It was around the year 2000 that e-Procurement started getting promoted as an alternative methodology for conducting public-procurement. Initially, the emphasis of Government and Multilateral Agencies promoting e-Procurement was mainly on transparent display of Tender-Notices and Tender-Documents. The focus gradually shifted to e-Bid-Submission and Opening (which was the electronic equivalent of sealed-bid tendering and its public-opening), and other forms of e-Procurement.

While discussing the subject of e-Procurement, it is important to appreciate the difference between its various forms. Broadly, e-Catalog or e-Marketplace is essentially for purchase of standardised low-value commonly-used items; e-Procurement or e-Tendering is generally referred to in the context of the electronic equivalent of the traditional sealed-bid tendering; e-Reverse Auction is a more open form of bidding (where the bids are not sealed), and is typically used for creating an open competition on 'price' for commoditized items or where technical and other criteria have been separately evaluated through sealed-bid e-Tendering.

In terms of the 'value of public-procurement' and its consequent 'sensitivity from audit perspective', the highest importance has to be given to e-Tendering/e-Procurement.

Benefits of e-Procurement (Myth vs Reality)

Potential benefits in terms of enhanced efficiency are well accepted. However, the projected benefits pertaining to enhancing Security, Transparency, Accountability and overall Integrity of the public-procurement process are contingent upon the design of the e-procurement application software, and other security measures.

Examples of Possible Malpractices

Technology is a dual-edged sword. In fact, without **adoption of appropriate precautionary measures, technology-enabled malpractices in e-procurement can be worse than in manual-tendering**. For example,

- Bid-Confidentiality can be compromised (by stealing bid-data and sharing it with a conniving vendor)
- Transparency related established practices for Public Bid-Opening can be compromised, et al.

Furthermore, in practice many such technology-enabled violation may **neither get discovered nor reported.** Keeping in view the principle of 'prevention is better than cure', it would be incumbent on regulatory authorities to proactively put in place preventive security and other remedial measures (Kohli, 2012, 2015).

Audit of e-Procurement Systems

Without going into various aspects of 'Audit of IT Systems deployed for e-Government' (see Kohli, 2017), it would be important to check if the e-Procurement systems are:

- Compliant with the relevant Governing/ Regulatory Framework
- Whether such systems have undergone a 'Certification' process to meet legal, security, technical/ conformity assurance levels

In the context of India, the most important document relating to the governing framework is the 'Quality requirements of eProcurement Systems dated 31st August 2011' (commonly referred to as DIT-Guidelines or DeitY-Guidelines or MeitY-Guidelines) issued by Standardisation Testing and Quality Certification (STQC), Department of Electronics and Information Technology (DeitY), Ministry of Information Technology, Government of India. These DeitY-Guidelines encompass relevant guidelines of the Central vigilance Commission (CVC) (as Annexure-II of the Guidelines); the GFR (as Annexure-III of the Guidelines); the IT Act 2000 (as Annexure-IV of the Guidelines).

As far as the 'certification' process is concerned, the CVC vide its circular dated 12th January 2012, and the Finance Ministry vide its Office-Memorandum dated 3rd September 2012, had directed that all e-Procurement systems used by Government entities in India should be certified for compliance with DeitY-Guidelines by STQC only.

Reality on the Ground:

While DeitY-Guidelines are very comprehensive in respect of ensuring Security, Transparency and Accountability in e-Procurement systems, **'enforcement' is still far from satisfactory**. Some disturbing aspects of the reality on the ground are as follows:

- Many large government-entities continue to use e-Procurement systems, which have repeatedly failed to get certified by STQC for compliance with DeitY-Guidelines.
- There are cases where STQC certification has been obtained, but the functionality of the e-procurement system as actually deployed is quite different from the prescriptions of DeitY-Guidelines. Just as the 'Volkswagen Emissions Scandal' (September2015) had exposed, even certification/ testing processes can be defeated by delivering in the real-world a product which is different from what was offered for certification (Kohli, 2016).
- As anticipated in the DeitY-Guidelines, due to the vulnerabilities relating to Bid-Confidentiality existing in some e-Procurement systems, it is understood that there is already some kind of e-tendering link in operation in some places, which can help favoured bidders to know competition-prices in a large tender (15-30 minutes before the 'deadline for bid submission'), and to help them change their bids suitably.

  Et al.

To assist the audit team in their endeavour to ensure 'Integrity' in e-procurement systems,a sample checklist is presented below.

Sample Checklist for 'Audit of some Critical Aspects of e-Procurement Systems'

Suggestions outlined in the checklist are essentially based on prescriptions given in the DeitY-Guidelines.

Overall/ General

1. It is mandatory for "the complete e-procurement system, viz the application along with the server in a specific hosting environment" to be certified by STQC for compliance with 'DeitY-Guidelines. In other words, if a Service Provider has set

up four separate e-Procurement portals for four different Government organizations, then each of these four portals has to be independently certified by STQC for compliance with DeitY-Guidelines (even if the same version of the application software has been deployed on all the four portals).

[Relevant regulatory references: CVC Circular dated 12th January 2012; Finance Ministry's Office Memorandum dated 3rd September 2012; section 6.0 of DeitY-Guidelines]

Points to be noted:

(a) Check whether there is a 'valid STQC certificate for compliance with DeitY-Guidelines' for the specific e-procurement system being audited. [If not, it is a 'Red-Flag'. Needless to state, the following scenarios could be straightaway 'Red-Flagged':

(i) e-procurement portals which have not been certified

(ii) where during the audit, a draft or discarded version of DeitY-Guidelines with a different date (ie different from 31st August 2011) is being referred to

(iii) Where a different STQC certificate (ie not specifically for compliance with DeitY-Guidelines) is being presented to mislead the auditors and users. (Note: Apart from certification for compliance with DeitY-Guidelines, STQC does testing and certification of many other types, such as OWASP etc.)

Further, if the following 'checks' are 'not true', it is a 'Red-Flag' --

(b) Whether the URL of the portal given in the STQC certificate is the same as that of the portal being audited. [There are instances where vendors have got one portal certified, and are displaying that certificate for all their other portals]

(c) Whether 'version reference' of the software solution of the portal is the same as that given on the related STQC certificate.

(d) Whether the 'portal is owned and operated' by the same entity with which the Government Buyer (ie purchasing-entity) has signed the contract for e-Procurement services. [For example, a Government Buyer may have been misled into believing that the Government entity with which they are signing the contract (especially on nomination basis) is the 'owner and/ or operator' of the portal and is responsible for the 'security of the database', while in reality the actual physical portal may be 'owned and/ or operated' by a private entity']

2. **To prevent misuse by the e-Procurement service provider, the service provider 'should not have access to the source code' of the e-Procurement software/ solution.** *[Service provider should carry out its activities with compiled code.]*

   [Relevant regulatory references: page-17 of DeitY-Guidelines]

3. **To prevent misuse by the e-Procurement service provider, the e-Procurement service provider or the portal operator should not be selling or providing PKI encryption and decryption certificates/ keys to the users of the portal.**

   [Relevant regulatory references: Annexure-I (section 2.1) of DeitY-Guidelines. On pages-19 & 25 it is stated, "Copy of the decryption-key (ie private key of the encryption certificate issued by a CA) is generally available (ie backed up) with the CA. Duplicate can generally be requested in case of loss, however, this can also be misused."]

Some Critical Functionalities

IMPORTANTLY, as stated earlier, even a 'valid STQC certificate for compliance with DeitY-Guidelines' may only be a 'facade cover up', and the actual

functionalities of the software deployed on the e-procurement portal may be different from the functionalities prescribed in the DeitY-Guidelines.

Cautionary Note: To get at the truth, the auditing team could themselves conduct some 'functionality checks' on the actual portal deployed in the field (and not on some demo portal). The user-manuals (for both Buyers and Suppliers) should also be independently procured and studied by the auditing team. Only then there is a reasonable chance for the truth to be revealed. Due to constraint of space, only some critical functionalities are being discussed here.

1. **Bid-Encryption Methodology:** This is the most critical functionality to be checked, as any compromise in Bid-Confidentiality before the 'online public tender opening event' will make a mockery of the public-procurement process. Section 3.1 of Deity-Guidelines requires that 'Bid Encryption' should be done at client end (i.e. bidder's computer) using Symmetric-Key, or Asymmetric-Key (PKI based) subject to issues raised in Annexure I and II of DeitY-Guidelines being suitably addressed. In addition, bids before transmission from the bidder's computer should be protected with SSL (now called TLS) encryption. Further, as prescribed in Annexure-I (section 3.2) of DeitY-Guidelines, "... at no point of time the System Administrator or Data Base Administrator should be authorized to hold the private (decryption) key."

Functionality to be Checked	Inference/ Conclusion
Is the main bid encryption being done at the client-end or database-level (ie server end) **Note:** A scenario, where bids before being transmitted from the bidder's computer are protected with only SSL/TLS Encryption, and Database-level Encryption is done before the bid is stored in the Database Server, is covered by Annexure-I (Section 3) of DeitY-Guidelines on pages 25-27. As per section 3.1 and Annexure-I (section 3) of DeitY-Guidelines, this method of database-level encryption (irrespective of whether symmetric or asymmetric key is used) is not acceptable as it violates the requirement of bid-encryption at client-end (i.e. bidder's computer) followed by SSL/ TLS encryption before transmission from the bidder's computer.	*If the main bid encryption is not being done at the client-end, it is a 'Red-Flag' as per DeitY-Guidelines --section 3.1; Annexure-I (sections 3.1, 3.2); Annexure-II (12);*
Assuming that Bid-Encryption is being done at 'Client-end', we have the following Scenarios:	
Scenario-1: Where asymmetric encryption methodology using Public-Key/ DSC or Encryption Certificate of an officer of the Buyer organization, or any other Public-Key specified by the Buyer organization is used for bid-encryption	
Security vulnerabilities of this form of bid-encryption are explained in Annexure-I (Section 2.0) of DeitY-Guidelines on pages 19-25. To mitigate the security risks mentioned in DeitY-Guidelines, it should be checked as to which of the following remedial measures (as given on pages 23-24 of Deity-Guidelines)has been adopted in the portal being audited: i) Key-Splitting ii) Repeated/ Multiple encryption iii) Any other Detailed information should be sought from the service provider as to how the security risks mentioned in section 2.0 of Annexure-I of DeitY-Guidelines have been satisfactorily addressed. Further, even if these	*If neither key-splitting, nor multiple repeated encryption, nor a better measure has been adopted, then this is a very serious 'Red-Flag'.* *If some of the remedial measures have been implemented, then decision has to be taken based on the 'field-level practicability and efficacy' of the measure.*

Functionality to be Checked	Inference/ Conclusion
measures have been adopted, 'field-level practicability and efficacy' of the measure should be checked by the audit team. For example, if key-splitting has been done, then keeping in view the IT Act and other aspects -- • In how many parts has the key been split? • How is the key split done? • Even after the key is split into 'N' parts, will at least one original copy remain in un-split form? (If so, can it not be misused?) • How and where is the 'Original' key 'securely' stored/ escrowed? • How and where are the split key parts 'securely' stored/ escrowed? • How many split key parts are required to be put together for Bid-decryption? • (et al). Similarly, if some measure such as 'multiple encryption' has been adopted, and three copies of the same bid have been independently encrypted using a different key each time, then it is actually making the situation worse as far as ensuring security is concerned, as connivance of any one of the three key-owners can compromise Bid-Confidentiality. In contrast, if 'repeated multiple encryption' has been done sequentially, then while the security situation improves to some extent, the dependency on the presence of 'all the three key owners' during the public tender opening becomes necessary, thus worsening the situation from a practical angle.	
Scenario-2: Where asymmetric encryption methodology (Public key of a user of the Bidder organization) is used for bid encryption	
Security vulnerabilities of this form of bid-encryption are explained in Annexure-I (Section 2.6) of DeitY-Guidelines on page-25. **Note:** Apart from the reasons detailed in section 2.6 of DeitY-Guidelines, for decryption this method would entail the 'mandatory' physical presence (during the public tender opening) of the bidder's representative who is the owner of the corresponding private key. Hence it is not acceptable as per DeitY-Guidelines and the established principles of public-procurement.	*If this method has been adopted, it is a 'Red-Flag'.*
Scenario-3: Where symmetric encryption methodology (bidder-generated passphrase) is used for bid encryption	
Most security issues which are applicable for other forms of bid-encryption become irrelevant in this case (refer page-22 of DeitY-Guidelines). This view is corroborated by section 6.7 of the final report issued by the e-Tendering Expert Group (e-TEG) appointed by European Commission. A report titled 'Recommendations for Encryption Policy' issued by the Data Security Council of India (DSCI) reinforces this view. However, even in this method, DeitY-Guidelines rightly require a few checks to be done as described in Annexure-I (section 4.1) on pages 27-28. Check 4.1(c) has now been made mandatory by STQC.	*Decision has to be taken after checking that the few minor concerns have been suitably addressed.*

Functionality to be Checked	Inference/ Conclusion
Scenario-4: Where symmetric encryption methodology (system-generated password/ passphrase) is used for bid encryption	
DeitY-Guidelines have not bothered even to discuss this method in detail, presumably because by inference the security concern mentioned on page-27 of Deity-Guidelines becomes applicable in this case, viz – "It may be mentioned here that at no point of time the System Administrator or Data Base Administrator should be authorized to hold the private (decryption) key". If the symmetric key (used for encryption/ decryption) is generated within the system, a copy of the key will always remain in the system for decryption, and such a key will be accessible to the database administrator. Even if this method is modified to some extent, such as by taking a copy of the system-generated symmetric key and further encrypting it with the public key(s) of the tender opening officer(s) simultaneously (i.e. having hybrid-encryption at this stage), bid-confidentiality can still be compromised through connivance of such officer(s).	*If this method has been adopted, it is a 'Red-Flag', unless a fool-proof method has been implemented to prevent access of the system-generated key or password to the database administrator(s) of the system. Even in case of hybrid-encryption (especially the way it would have to be implemented in this case), connivance of the concerned officers cannot be ruled out.*
Notwithstanding the above Scenarios of Bid-Encryption Methodology, additional functionality checks relating to Bid-Encryption would have to be done as follows:	
Annexure-I (section 1.2) of the DeitY-Guidelines requires that – "Each bid part (e.g. technical, financial) may be required to be submitted in a 'summary format' along with a 'detailed bid'. The latter could be a large file. There should be provision of appropriate file size (at least 10 MB) in the application with data encryption as outlined elsewhere in these Guidelines. After having submitted the 'original' bid for each bid-part, a bidder has a right to submit: 'Modification' bid; 'Substitution' bid; Or 'Withdrawal' bid for all his bid submissions." The e tendering system must effectively cater to all these possibilities without compromising security and transparency in any manner at any stage, for any bid part(such as Pre-qualification, Technical, and Financial).The e-tendering system need to have templates to offer flexibility in bidding methodologies as prevailing and followed currently in the manual process. Further, system should have templates to adopt bidding methodologies as may be prescribed by respective authorities." The above requirements are reiterated in Annexure-I (sections 6.1 and 6.2) of the DeitY-Guidelines. Based on the above prescriptions, the following checks can be done:	
Is there a facility in the system of having a 'summary format' (i.e. a flexible electronic template) for the **prequalification envelope**?	*If any of these facilities is not available in the prescribed form, it is a 'Red-Flag'.*
If the above answer is 'Yes', is there a facility in the system of digitally signing, as well as, encrypting such a bid-part at the client-end using one of the permissible encryption methodologies (suitably augmented as discussed above)?	
Is there a facility in the system of having a 'detailed bid' (i.e. a file of at least 10 MB) for the prequalification envelope?	
If the above answer is 'Yes', is there a facility in the system of digitally signing, as well as, encrypting such a bid-part at the client-end using one of the permissible encryption methodologies (suitably augmented as discussed above)?	
Is there a facility in the system for 'Modification' of the prequalification envelope?	
If the above answer is 'Yes', is such a modification-bid suitably encrypted and digitally signed before submission?	

Functionality to be Checked	Inference/ Conclusion
Is there a facility in the system for 'Substitution' of the prequalification envelope?	
If the above answer is 'Yes', is such a substitution-bid suitably encrypted and digitally signed before submission?	
Is there a facility in the system of having a 'summary format' (i.e. a flexible electronic template) for the **technical envelope**?	
If the above answer is 'Yes', is there a facility in the system of digitally signing, as well as, encrypting such a bid-part at the client-end using one of the permissible encryption methodologies (suitably augmented as discussed above)?	
Is there a facility in the system of having a 'detailed bid' (i.e. a file of at least 10 MB) for the technical envelope?	
If the above answer is 'Yes', is there a facility in the system of digitally signing, as well as, encrypting such a bid-part at the client-end using one of the permissible encryption methodologies (suitably augmented as discussed above)?	
Is there a facility in the system of having a 'summary format' (ie a flexible electronic template) for the financial envelope?	
If the above answer is 'Yes', is there a facility in the system of digitally signing, as well as, encrypting such a bid-part at the client-end using one of the permissible encryption methodologies (suitably augmented as discussed above)?	
Is there a facility in the system of having a 'detailed bid' (ie a file of at least 10 MB) for the financial envelope?	
If the above answer is 'Yes', is there a facility in the system of digitally signing, as well as, encrypting such a bid-part at the client-end using one of the permissible encryption methodologies (suitably augmented as discussed above)?	
Is there a facility in the system for 'Modification' of the **Financial envelope**?	
If the above answer is 'Yes', is such a modification-bid suitably encrypted and digitally signed before submission?	
Is there a facility in the system for 'Substitution' of the Financial envelope?	
If the above answer is 'Yes', is such a substitution-bid suitably encrypted and digitally signed before submission?	
Is there a facility in the system for 'Withdrawal' of the submitted bid by the bidder with his digital signature?	

2. Online Public Tender Opening Event: This is another critical functionality to be checked, as this event is the backbone of 'Transparency' in public-procurement. It is important to note that an 'Online Public Tender Opening Event' is different from a mere 'Online Tender Opening Event'. While the former type, if sincerely implemented and conducted in the 'simultaneous' and 'interactive' online presence of bidders in an elaborate manner ensures proper 'Transparency', the latter type has the potential of being a mere 'eyewash'. Annexure-I (section 6.3) on pages 35-38 of DeitY-Guidelines describes the issues and requirements in reasonable detail and should be thoroughly perused. Other sections of the DeitY-Guidelines, such as - Annexure-II (checkpoint 8 on page-45), Annexure-III (pages 54, 60, 63, 64, 68, 69) are also relevant. Some recommended checks are as follows:

Functionality to be Checked	Inference/ Conclusion
Is there an Online Public Tender Opening Event conducted in the 'simultaneous' and 'interactive' online presence of bidders? Where the answer to the above question is 'Yes', the following questions should be asked: Are the bids opened in the simultaneous online presence of the bidders? Note: Merely opening bids online, and then subsequently displaying some results to the bidders does not fulfill the requirements of a transparent Online Public Tender Opening. Is there are a proper online attendance record of the authorized representatives of the bidders, as well as, the Tender Opening Officers authorized for that tender? Is the opening of the Online Virtual Tender Box distinct from opening of the bids? Is there facility for one-by-one opening of the sealed bids in the simultaneous online presence of the bidders? Is there facility for performing Online Security Checks to assure bidders of non-tampering of their bids, during the online TOE itself? **Note:** A prerequisite for such a facility is that bidders should be able to 'interact online' with the TOE officers in a transparent manner during the event itself which is visible online to all participants. Is there facility for Online verification of the digital signatures of bidders affixed to their respective bids? Is there facility for reading out, i.e. allowing bidders to download the electronic version of the salient points of each opened bid (opened in the simultaneous online presence of the bidders)? **Cautionary Note:** In some systems, while the bidders are allowed to login for witnessing the opening event, they are essentially mute spectators. Bidders cannot participate interactively. Furthermore, the data of the opened bids is posted subsequently, sometimes after many days, and for certain bid-parts it is not posted at all! In such situations there is obviously tremendous potential for indulging in mal-practices. Is there a procedure for seeking clarifications by the tender opening event (TOE) officers during Online Public TOE from a bidder in the online presence of other bidders, and recording such clarifications?	*If this facility is not available in the prescribed form, then this is a serious 'Red Flag'.* *If any of the required facilities is not available in the prescribed form, it is a 'Red-Flag'.*

Functionality to be Checked	Inference/ Conclusion
Note: A prerequisite for such a facility is that bidders should be able to 'interact online' with the TOE officers in a transparent manner during the event itself which is visible online to all participants. If there feature of digital counter signing (by all the tender opening officers) of each opened bid, in the simultaneous online presence of all participating bidders? If there facility for generation of the 'Minutes of the Tender Opening Event' and its signing by the concerned officers in the simultaneous online presence of the bidders? Can the Tender Opening Officers be changed at the last moment without jeopardizing the conduct of Online Public Tender Opening Event, and without using the 'decryption key / digital signature key' of the absent officers? While bidders should be welcome to be present physically during the TOE, it should not be mandatory for them to do so.	

Other Important Functionalities

Checks similar to those delineated above have to be developed and conducted for other important functionalities relating to e-procurement, such as –Password-Generation and Storage, Authentication of Electronic-Records, Facilitation of various Types of Bidding-Methodologies, User Organization's Virtual Administrative Hierarchy, Audit-Trails, et al. Due to constraints on the size of the article, these aspects are not being covered here.

Snippets

1. **Why did the computer keep sneezing?**
   Answer - It had a virus!
2. **What is a computer`s first sign of old age?**
   Answer - Loss of memory.
3. **What happened when the computer fell on the floor?**
   Answer - It slipped a disk

REFERENCES:

i) e-Tendering Expert Group (e-TEG) appointed by the European Commission (2013). Recommendations for Effective Public e-Procurement, Part II: Operational Recommendations. [Online]. Available at http://ec.europa.eu/internal_market/publicprocurement/docs/eprocurement/eteg/eteg_part2-operational_recommendations_en.pdf. [Retrieved March 30, 2016]

ii) Kohli, J. (2012). Red Flags in e-Procurement/ e-Tendering for Public Procurement and Some Remedial Measures. Paper presented at the IPPC5 at Seattle, USA. [Online]. Available at http://www.ippa.org/IPPC5/Proceedings/Part2/PAPER2-6.pdf [Retrieved April 6, 2016]

iii) Kohli, J. (2015). "Combating Organized Corruption in Public-procurement Through Appropriately Designed e-Procurement Systems''. Paper presented at the Third Conference on Evidence-Based Anti-Corruption Policies (CEBAP III) on Organized Corruption', organized by Thailand's National Anti-Corruption Commission (NACC) in collaboration with the World Bank et al., Bangkok, Thailand, June17-18, 2015.

iv) Kohli, J. (2016).Avoiding the Volkswagen Emissions Scandal in E-procurement Systems: Imperative of Transparent Disclosure Norms and Certification of Critical Functionalities. Paper presented at the IPPC7 at Bali, Indonesia, August 4-6, 2016.

v) Kohli, J. (2017). "Integrity Issues in ITSystems (IT Audit Perspective)". Presentation made at the 'International Centre for Information Systems & Audit (iCISA)' of the Comptroller and Auditor General of India in November 2017.

vi) STQC Directorate (2011). Guidelines for Compliance to Quality Requirements of eProcurement Systems (Issued on 31st August 2011 by DeitY, Ministry of Communications and Information Technology, Government of India). [Online]. Available at http://www.stqc.gov.in/sites/upload_files/stqc/files/Guidelines-for-Compliance-to-Quality-Requirements-of%20e-Procurement-Systems.pdf[Retrieved March 30, 2016]

Theme Article

Data – Privacy concerns in Information Technology

Compiled by: M.P. Hemantha Kumar, Administrative Officer

On the 24th of August 2017, a nine-judge bench of the Supreme Court delivered its verdict in Justice K.S. Puttaswamy vs Union of India, unanimously affirming that the right to privacy is a fundamental right under the Indian Constitution. In the era of social media, where all the personal details are shared with literally the whole world in seconds freely and casually, does this right even impact us as citizens?

Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others. In USA, the ***right to privacy*** refers to the concept that one's personal information is protected from public scrutiny. U.S. Justice Louis Brandeis called it "the right to be left alone." Control over one's ***personal*** information is the most fundamental freedom that an individual can have.

In the present world, the smart mobile devices have completely altered the perception of concept of privacy, as the user does not seem to be bothered about the way, personal information is being tracked and viewed. These devices are being designed and refined to address the needs almost all the needs of the individuals, be it buying articles, to do banking and financial transactions, using the mobile for navigation or even for office working like checking our emails, editing documents etc., The list can go on. In a nutshell, a mobile user today gets what he wants when he wants and the way he wants.

Emerging Risks

Privacy concerns are one the Emerging risks, due to the emergence of Social Networking, Mobile computing, End user computing, Cloud computing and malware applications in the Technology sphere.

Each of us is involved in our routine, day to day activities with these applications, either consciously or unconsciously. It is a fact that almost every one of us would have used and continue to use free applications in our mobiles, using emails without even knowing where and in which location our data is stored.

The Present Scenario

A truism which is popular among privacy advocates is that:

If you are not paying, you are the product

One's age, interests, purchasing habits, frequented locations, health, and social map are all valuable pieces of information that comprise a digital shadow of a user, which can be packaged, bundled, and sold to the highest bidder.

Consider flashlight apps. They are meant to do one simple thing: turn on the LED flash of mobile phones. But many ended up having access to a lot of unnecessary data and phone functions, including users' calendars, location, and camera. The infamous “The Brightest Flashlight” app shared users' precise location and unique device identifier to third parties without disclosing that it did so—not exactly critical to a functioning flashlight.

Profile of Author

M. P. Hemantha Kumar, is a B.Sc (Physics), MA (Public Administration), MA (Mass Communication and Journalism), Masters in Computer Applications, Masters in Business Administration, ICWA (Inter), CISA, CISM. He has international exposure in the field of IT. Currently pursuing law he is passionate about computer security, privacy and the laws relating to the protection of individual data.

Facebook has many users across the world and it generates its revenue through advertising, whereby, advertisers can use the wealth of personal data about users from Facebook's product ecosystem for their product promotions. For its part, the Menlo Park, California based company claims that it makes the data anonymous and serves the information to advertisers in custom demographic buckets. This in fact implies that the users' digital footprints and personal data are being used to generate revenue.

Recently it has also emerged that Facebook apps on mobiles routinely collect call and text histories of users. Not many know this neither are they overtly concerned. The point is, shouldn't they be concerned?

Further, the recent expose by newspapers in America that Cambridge Analytica a private firm, was using the private Facebook data of tens of millions of users to map and sell psychological profiles of American voters to political campaigns, has thrown the much needed spotlight on data harvesting, security and privacy in the digital world.

Uber, for instance, requires access to your location data even when you are not using it unless you turn off location data entirely on your phone. The question is why they would need it at all.

In 2014, the Starbucks app was found to be ***storing passwords, email address, and previous GPS information unencrypted,*** leaving it open to onlookers to exploit. Starbucks ***addressed this vulnerability*** shortly after it was discovered, but it is certainly not the only app to have had this issue.

Safety Risks

We generally assume that the hardware and software which we buy or bought, or the application which we installed are perfectly safe and will protect our data and our privacy. But recent instances in the public news, throw a pointer to the fact that our assumptions may not turn out true always.

Oops... Some HP Laptops Shipped With Hidden Keylogger

December 12, 2017

Some HP laptops users came with a preinstalled program to capture the keystrokes of users, a security researcher recently discovered. The researcher, Michael Myng aka "ZwClose," discovered the keylogger software while trying to solve a keyboard problem for a friend. The software is turned off by default. After Myng contacted HP about the program, it quickly released a patch to get rid of it.

A case recently emerged wherein Hewlett Packard had shipped laptops with hidden key logger software.

With the advent of Data Analytics, it is necessary for every company to have the user information, in terms of location, age, and what their job details, in order to profile them and analyze what their interests are, so that they can make money.

Facebook Phone-Scraping Takes Users by Surprise

March 27, 2018

Facebook on Sunday confirmed that its Messenger and Lite apps for Android smartphones routinely collect call and text histories. The call and text history logging are opt-in features for people using Messenger or Facebook Lite on Android devices, the company said in a post. The feature is designed to help users stay connected, and it improves the Facebook experience, according to the company.

Google, for instance has collected so much of user information, that it even can change how the search engines throw results or block certain search results.

Privacy Risks

Most of us not only use mobiles, but are also contributors to the next biggest word in internet, Cloud Computing. Say for example, we use emails pretty much without consciously understanding where exactly is the email data stored or in which part of the globe exactly it is stored, who has access to it or how secure it is. Are the companies' policies secure enough to prevent manipulation and misuse of our data?So, where exactly does these privacy risks lie?

a) The biggest looming concern is for organisations, where employees configure their company emails on their mobile. What this effectively does is, that without the employees' knowledge other apps in the mobile, which have already got access during installation, can snoop on the business and the employee emails.

b) Compromised banking passwords and sms data.

c) Private photos on mobile getting stored in the cloud, with the user having little or no control. Inability to access or delete the digital trail in the internet.

Data in the hands of organisations is wealth generator. Information is the business of these organisations. So addressing these risks, would require the Government as a protector of the citizens' rights to step in, by enactment of laws governing data storage and by setting standards on the need for access of user data and its use by software developers and applications. For example, Google has a separate webpage for request for removal of content indexed on Google Search based on data protection law in Europe, whereas the same is not the case in many other parts of the world.

The organizations and business entities need to have clearly spelt out policies and rules in regulating employees accessing company mails through mobiles, and educating employees of the risks involved. Lastly but not the least, the private users, who contribute to the millions being made by the private companies, by just giving their data for free, should be educated and made aware of the risks involved in installing applications which seek all types of permissions and need to be more aware about their privacy rights.

REFERENCES:

i) https://www.technewsworld.com

ii) www.livelaw.in

iii) http://www.slate.com/articles/technology/future_tense/2017/02/how_to_understand_what_info_mobile_apps_collect_about_you.html

iv) https://www.digit.in/internet/vulnerability-in-maadhar-android-app-allows-anyone-to-steal-your-aadhar-data-finds-french-security-r-39086.html

v) Read more: How Does Facebook Make Money? | Investopedia
https://www.investopedia.com/ask/answers/120114/how-does-facebook-fb-make-money.asp
Follow us: Investopedia on Facebook

Sneak Peek

Wearable Technology

Wearable technology is one of the digital trends. Wikipedia defines wearable technology as smart electronic devices (electronic device with micro-controllers) that can be worn on the body as implants or accessories. The concept of wearables is not as new as one might think. Back in the 17th century, one pioneering designer in China created a functioning 'smart ring' Zhusuan featuring a 1.2cm long, 0.7cm wide abacus that sits on the finger. Developed in the Qing Dynasty era (1644-1911), the origins of the ring are unknown. However, the beads are far too small to be moved using fingers. Therefore, the ring', or China's abacus, has seven rods with seven beads on each rod. Despite its small size, the rings still worked as a counting tool.

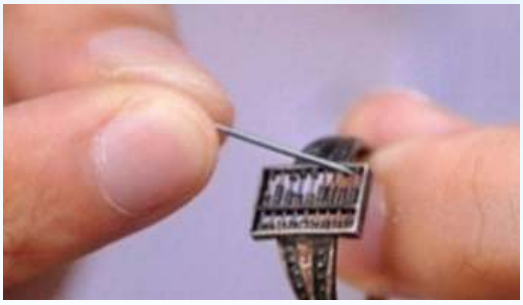


Image source: www.wearable.com

Image source; www.wearable.com

Wearables are becoming mainstream and disrupting almost every industry, with the biggest impact being seen in consumer durables, healthcare, defense, manufacturing etc. It appears prominently in consumer electronics with the popularization of the smart watch, fit bits and activity tracker.

Of the whole wearable device market, medical devices are the biggest field followed closely by fitness aids. Wearable technologies in healthcare are growing in rapidly with companies such as Google, Apple and Samsung allocating vast resources on researching various kinds of medical wearable devices.

Wearables continue to evolve as virtual reality applications provide experience-based applications for clinicians and patients. Doctors, specifically surgeons, have been quick to adopt wearables such as Google Glass. They are now able to preload CT and X-ray images. To be able to have those X-rays directly in one's field without having to leave the operating room or to log on to another system elsewhere, or to turn oneself away from the patient diverting attention, is very helpful in terms of maintaining the doctor's attention where it should be, which is, on the patient 100 percent of the time.

On the patient side, Zephyr Anywhere's BioPatch is an FDA-approved (U.S. Food & Drug Administration) , small device that is attached to a patient's chest monitoring their vitals minute-by-minute and collecting medical-grade data for doctors' use. Typically, patients are checked on every 4-8 hours, which is not always ideal for the amount of attention each patient needs. The BioPatch alerts nurses via smartphones, giving them the ability to be more efficient in prioritizing patients. The BioPatch monitors patients 24 hours a day. Patients with serious illness can wear them home, and it can notify the hospital of any bad signs.

Wearables are also starting to be more widely adopted in aerospace and defense, and this trend is likely to pick up momentum during the next few years as the technology continues to mature. Wearable technology provides instant access to critical information, improves quality, and helps increase collaboration. This technology enhances existing workflows and opens new opportunities in many aspects of this industry.

In Defence, army researchers are exploring the use of a wearable arm band sensor to convey the meaning of standard infantry hand signals to intelligent communication software and facilitate information dissemination and retrieval. Wearable

antennas can be confining - not only to the war fighter's comfort in the field, but also to the RF (Radio Frequency) communications bandwidth the war- fighter can use.

The Crystal Group TAC-V integrated military communications system for mobile computing capability is small and lightweight for infantry and vetronics applications. Today's tactical air control parties, which help guild precision-controlled weapons to their targets, are making some use of wearable electronics.

Wearable technology pioneered by the aviation sector included oxygen masks, radio headphones and helmets, G-suits and electrically heated clothing – all necessities developed as aircraft flew faster & higher. Wearable monitoring validates a new cloth vest that monitor astronaut's heart rate and breathing patterns during sleep. It collects data to investigate whether changes in heart activity are related to astronauts' poor sleep quality. NASA's X1 robotic exoskeleton, is the robot a human can wear over his or her body to either assist or inhibit movement in leg joints. The technologies developed for the exoskeleton and the Space Suit to help with rehabilitation and augmentation of one of the most complex human joints, the shoulder. The Soft Wearable Upper Extremity Garment, or "Armstrong," is worn on the upper body and can activate the shoulder and elbow joints using a Bowden cable transmission system. This system uses actuators on the torso to pull on synthetic tendons that cross the shoulder and elbow joints to create the desired movements.

The true potentials of the wearables is not having screens on the wrist but rather having new and interesting sensors which means new data and new data means new insights and new insights means new application for the wearable industry, which is set only on the path of forward program.

https://www.gocomics.com/comics/lists/1720511/social-media-comics

REFERENCES:

i) https://www.militaryaerospace.com/articles/print/volume-27/issue-9/special-report/wearable-electronics-adapt-to-the-infantry.html https://www.nasa.gov/feature/nasa-s-newest-wearable-technology-takes-on-the-human-shoulder https://www.nasa.gov/mission_pages/station/research/experiments/1279.html

ii) https://www.aerosociety.com/news /wearables-the-next-frontier-for-aerospace/

iii) https://sightcall.com/wearable-tech-taking-healthcare-industry/

iv) https://www.sciencedaily.com/releases/2016/09/160912132730.htm

iv) https://thegadgetflow.com/portfolio/hands-free-assistive-device/

v) https://thegadgetflow.com/portfolio/ personal-noise-blocking/

App Watch

Let us take a look at a few apps which helps increase the productivity and Time Management of the Employees

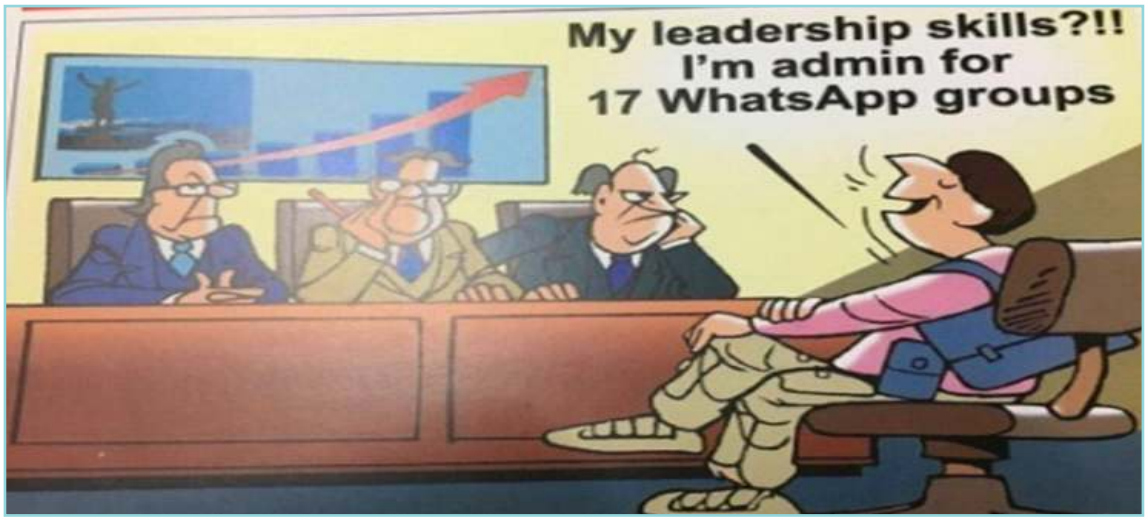
Keka's GPS & Mobile Attendance Management Software for field staff

Keka's GPS and mobile attendance management software is fully integrated with biometric attendance and shift management, designed to monitor. This feature is one of a kind in the Indian market and tracks an employee's location through their smart phone. It also seamlessly integrates with Keka's payroll software. The staff just need to log in to their mobile devices and start recording the working time, along with the location being automatically tracked. This app can track time and coordinate the best of information available even when offline.

Rescue Time Management - App

Rescue Time helps one manage the computer and mobile time. It is a fully automatic productivity tracker that can track time on the computer, time spent on websites, and mobile screen time. This app enables accurate automatic time tracking of one's mobile apps, setting goals for one's digital life, reports the voice call time, know where the web site time is spent and see how one's digital habits change over time. All the time spent on the computer is automatically categorized and ranked by productivity level (distracting - neutral - productive) and a weekly summary report giving an overview of the logged time is generated. Full reports and charts–along with goals, alerts, and lots of other features–are available via this web app

https://www.timesofindia.indiatimes.com - cartoon by Ajit Ninan



Emerging Opportunities and Risks in Cryptography: A Case of Aadhaar based E-signing

Compiled by: Nanda Dulal Das, Dy. Accountant General

Introduction

Cryptography is the science of encrypting and decrypting sensitive data or information in a secure manner which cannot be deciphered except by the intended recipient. Digital Signatures are tools which operate on the principles of cryptography seeking to ensure four major criteria while storing or transmitting documents over a network: confidentiality, i.e. keeping the information secret from the unauthorized users; data integrity, i.e. non-alteration of transmitted data; authentication, i.e. identification of the sender is confirmed and non-repudiation, i.e. the senders cannot claim ignorance of his act of signing. Digital Signature can be defined as a signature-code attached to an electronically transmitted document to verify its contents and sender's identity.

This paper seeks to study how digital signature has gained importance at present and how a paradigm shift has occurred with the introduction of Aadhaar-based e-signing resulting in removal of barriers towards electronically signing any documents. Further, this paper also seeks to foresee the kinds of risks and difficulties which may be encountered in different government and non-government organizations during its implementation.

Digital Signature and its Legal Status in India

Digital Signature operates on the principle of using two security keys for encryption and decryption of information. If both the encryption and decryption is to be done using a single private key, the same is categorized as symmetric cryptographic technique, while in asymmetric cartographic technique a private key is used by the sender to encrypt the information and the intended receiver uses the public key received with the signed documents to decrypt the information. This technique is widely used because of advantage of having public key widely shared while the private key keeps the signers' identity intact. Generally, cryptographic tokens are used for generation of digital signature and it is then transmitted to the intended user through a secured network.

Since 'paperless office' and 'prompt delivery of services' have become increasingly important for both government and non-government organizations delivering services by use of digital signature is on the rise in service-delivery organizations. While use of Digital Signature in non-government sphere in India had started well before the dawn of the millennium, Article 3 of the Information Technology Act, 2000 had legalized the use of 'Digital Signature' which was to be created and verified by cryptographic techniques.[i][ii] Section 5 of the IT Act, 2000 gives legal recognition to digital signatures based on asymmetric cryptosystems. Thus, digitally signed

Profile of Author

Mr. Nanda Dulal Das did his M. Phil on "Dynamism of Agricultural Land-Use around Metropolitan Cities with a special focus on Delhi" and Ph. D. on "Convergence between Natural Resource Based Livelihood Programmes: A Case Study of Watershed Development Projects & MGNREGS" in India, from Jawaharlal Nehru University, New Delhi in the year 2009 and 2014 respectively. Mr. Das had extensively used techniques of Remote Sensing and GIS in his research. Mr. Das has worked at different times in Vidyasagar University, West Bengal Civil Service and Indian Defence Accounts Service before joining the IA&AS.

documents are treated at par with the paper based documents.[iii] In 2001, when the 'Model Law on Electronic Signature' was adopted by the United Nations Commission on International Trade Law (UNCITRAL)[iv], necessary amendments (in 2006 and 2008) in the IT Act, 2000 have been brought in for harmonization with the Model Law to provide for alternative technologies for the purpose of electronic signature. Digital Signature can also be legally upheld in the Court of Law, as Section 10A of the Information Technology (Amendment) Act, 2008 lays down clearly that when an agreement is "expressed in electronic form or by means of an electronic record, such contract shall not be deemed to be unenforceable solely on the ground that such electronic form or means was used for that purpose"[v].As of now, for signing a document digitally, every user is required to obtain a Digital Signature Certificate (DSC) from a Certifying Authority (CA) licensed by the Controller of Certifying Authorities (CCA) under the Information Technology (IT) Act, 2000.

Emerging Risks in use of Digital Signature

Multiple security risks need to be addressed before using Digital Signature. These risks mainly arise at three stages- a) signature creation, b) signature transmission and c) signature verification. Attackers or intruders try to invade the different stages and access unauthorised access to a document or make it look like signed by an authenticated signee. Six major aspects which the attackers would attempt, are as detailed below[vi]:

I) Environment manipulation
ii) Modification prior to signature computation
iii) Modification post signature computation
iv) Unauthorised invocation of the signing function
v) Compromise of the signature creation data and
vi) Influence on signature verification result

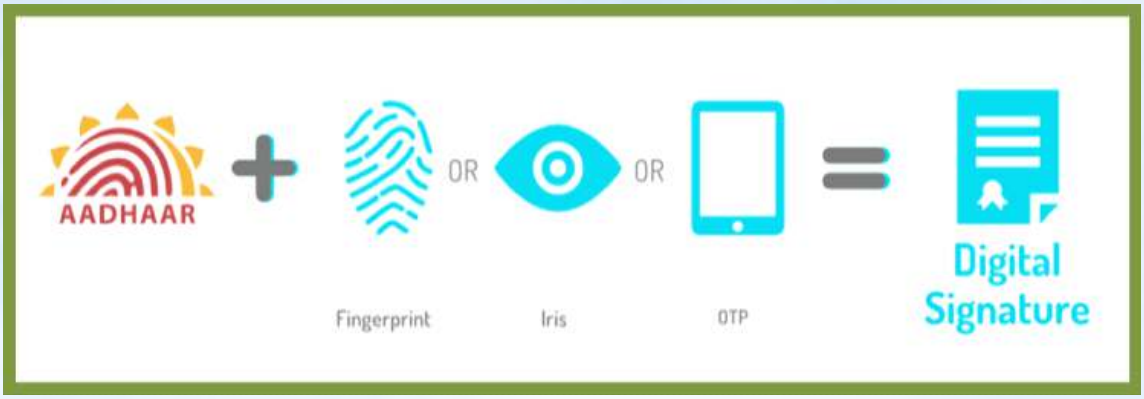
Hence, security experts and Certifying Authorities have a mammoth task for improvement in security at these many different stages.

Advent of Aadhaar-based e-signing

World's largest biometric programme, dubbed as "the most sophisticated ID programme in the world"[vii], Aadhaar is a 12-digit unique ID number provided to the citizen of India as a proof of identity. Since, Aadhaar is based on demographic as well as biometric data, i.e. finger-print and iris scan of the individual, it largely ensures that individual identity is not duplicated and this feature has impacted the way digital signatures are generated and used. In India, Aadhaar enrolment has reached almost its zenith with over 99% of its citizens being under its ambit[iiiv]. Government organisations, as service-providers, in their dealings with the citizens prefer to obtain the Aadhaar details for ensuring identical beneficiary selection and to avoid duplication in provisioning of services. Hence, Aadhaar enabled payment system (AEPS), Biometric Attendance System (BAS) etc. have become popular in wider parlance. To disburse wages under Mahatma Gandhi National Rural Employment Guarantee Scheme (MGNREGS) and pension payment through biometric authentication via smart cards, Andhra Pradesh became the pioneer almost a decade ago[ix]. While management of the biometric data and its misuse has been widely debated and figured in popular debate and Supreme Court's deliberations, the use of Aadhaar-based biometric data has become common place nowadays.

The present process of issuing digital signature involves physical appearance of the applicant before the CA, verification of identity and address of the signer through paper documents. Issuance of hardware cryptographic token has a disadvantage of scale in a country as big and as populated as India[x]. Aadhaar-base E-sign is a paradigm shift in this respect as it is based on e-KYC service, i.e. authentication of the signer can be done either through matching of fingerprints/ iris or through mobile-based One Time Pin (OTP) [Image I] and it is possible to digitally sign documents without obtaining any hardware cryptographic token.

Image : Aadhaar-based digital signature (e-signing)



[Source: Aadhaar API, as viewed on 8th March, 2017 from https://aadhaarapi.com/product/e-sign/]

Therefore, use of Aadhaar-based digital signature has provided an added advantage since the requirement and maintenance of individual digital signatures in separate cryptographic token can be dispensed with and documents can be e-signed from anywhere based on Aadhaar based authentication.

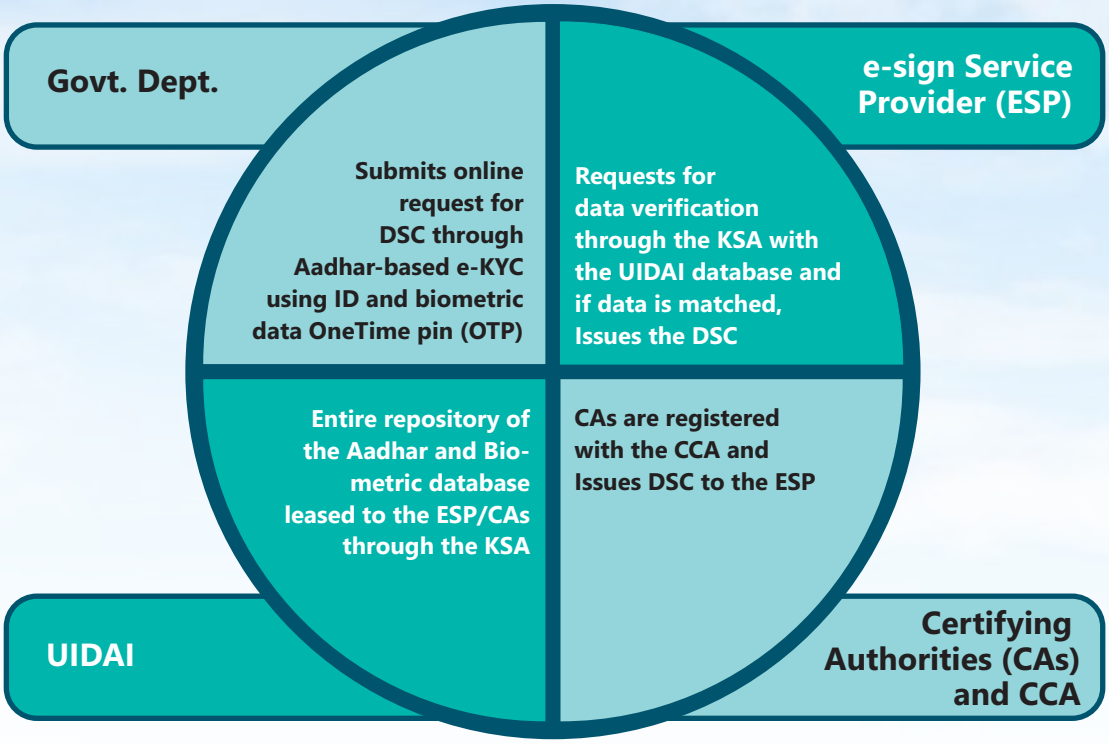
Introduction of Aadhaar based e- Signature in Indian Governance

Though Aadhaar-based service delivery had started mainly using biometric credentials for transferring benefits of social sector schemes to the beneficiaries, Govt. of India had introduced the Electronic Signature or Electronic Authentication Technique and Procedure Rules, 2015 in January, 2015 and modified the same twice subsequently[xi].It laid down seven set of requirements for e-authentication using Aadhaar e-KYC services like it required that applicable use of e-authentication, hash, and asymmetric crypto system technique as valid techniques for issuing DSC by the CA. DSC is issued by the CA after the electronically signed Form-C (which is simple form containing Applicant's name, address, details of organisation and mobile number), as verified with the Aadhaar e-KYC services and after receipt of consent of the applicant of the DSC. Since, the procedure involved in e-signature is almost identical with that of digital signature; the authenticity, integrity and non-repudiating features of the digital signature remain intact with respect to e-signature as well.

Main Stakeholders in e-Sign Service

Application Service Providers (ASPs) are the entity using the e-sign service and can be Government departments, Banks, private or public organizations. E-sign Service Provider (ESP) is a 'Trusted Third Party' as per IT Act, 2000 and is essentially a KYC User Agency (KUA) with the Unique Identification Authority of India (UIDAI). This service is generally accessed by the ESP through the e-KYC Service Agency (KSA) that establishes secure leased line connectivity with the Aadhaar database after approval from the UIDAI. Usually, ESPs are 'Certifying Authorities (CAs)'; licensed by the Controller of Certifying Authorities (CCA) or they have an arrangement with the CAs for issuance of Digital Signature Certificate (DSC).[xiii]

Image : Stakeholders and Process-flow in Aadhaar-based e-signing



Emerging Risks and Implications of Aadhaar-based e-KYC and e-Sign

Multiple stages of probable attack at different stages of digital signature has been enunciated in the earlier section. Some additional risks relating to privacy and security concerns in Aadhaar-based e-signing are highlighted here. Reports of leakage and misuse of Aadhaar data as seen in the recent past have deepened the fear on privacy concerns of millions[xii]. Aadhaar authentication verifies Aadhaar number along-with demographic and biometric data with the database of the Central Identities Data Repository (CIDR). When a person gives consent for Aadhaar authentication for obtaining certain services, he/she agrees to share certain data with the service-providing entity. This portion of data becomes vulnerable for unintended disclosure, if not properly secured by the entity. Starting from linking of PAN with Aadhar to linking of bank accounts, mobile numbers, investment portfolios etc. all have gradually been implemented which makes it probable that by collating data based on aadhar from different data repositories like the banks, tax department, business establishments, etc., one can access all personal, professional and financial details of an individual. This may lead to privacy concerns.

The IT Act, 2000 and Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 seek to protect sensitive personal information. However, they may have to keep pace with emerging cyber risks.

Securing the Aadhaar database is responsibility of the Unique Identification Authority of India (UIDAI). It also decides on the procedures of authentication. Hence, only UIDAI could take action in the event of any breach taking place. Further, Justice B. N. Srikrishna (Rtd.) Committee which is drafting a legal framework for data

protection is expected to remove the large scale privacy concerns existing at present with the use of Aadhaar[xiii].

As far as e-sign is concerned, it ensures privacy of the signer as it requires only the thumbprint (hash function) of the document to be submitted for signature function instead of the whole document. Hence, any additional risk to privacy because of adoption of Aadhaar based e-KYC verification for e-signing any document may not be significant, particularly when the Controller of Certifying Authorities (CCA) monitors the process of issuance of certificate. Nonetheless, the need is to make cautious use of this facility and to keep tab of all the uses of Aadhaar data, where consent has been given by the person concerned.

Concluding Remarks

Digitally signed authenticated electronic documents transmitted online have necessitated increasing security measures at different stages from pre-signature-generation to post-signature-verification stage. Despite the privacy and security concerns; Aadhaar-based e-KYC and e-Sign would streamline the outreach of the government as duplication of identity would largely reduce. The delay as experienced in movement of paper documents and in procuring the necessary hardware for conventional digital signature would also come down as the approval for obtaining private key for e-signing by the concerned person/official and e-signed documents are transmitted online. In a nutshell, it can be concluded that the era of Aadhaar-based service provisioning has widened scope for any person or organisation to adopt this e-sign technology as it would just eliminate the tedious process of obtaining conventional digital signature, retaining them and using them sparingly.

REFERENCES:

i) "Cryptography just for the Beginners", Tutorialspoint Simple Easy Learning, Copyright 2015 by Tutorials Point (I) Pvt. Ltd.

ii) "The history of the Signature", Legalsign Staff Writer (GB), 19 February, 2016 viewed 21st February, 2018 from https://legalesign.com/blog/history-of-signatures/

iii) Diffee W.. Hellman ME, (1976) "New Directions in Cryptography", IEEE Transactions on Information Theory, IT-22(6):644–654, Nov. 1976.

iv) Shellar Naveen, 2014, Digital Signature Laws in India, viewed 21st February, 2018 from http://www.iamwire.com/2014/09/digital-signature-laws-india/100694

v) SS 3A, The Information Technology Act, 2000.

vi) "Guidelines for Usage of Digital Signatures in e-Governance", Ver. 1, Dept. of Electronics and Information Technology, MEITY, GoI.

vii) UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001, United Nations, New York.

viii) "Global Guide to Electronic Signature Law: Country by Country Summaries of Law and Enforceability", Adobe Systems Incorporated, 2016.

ix) Ardieta, J. L. H. 2011, "Enhancing the reliability of digital signatures as non-repudiation evidence under a holistic threat model", Doctoral Thesis, University Carlos III of Madrid, Leganes.

x) World Bank gives Aadhaar thumbs up; wants other nations to adopt it too", The Business Standard, 17 March, 2017, viewed April, 2018 from http://www.businessstandard.com/article/economypolicy/world-bank-gives-aadhaar-thumbs-up-wants-other-nations-to-adopt-it-too-117031700241_1.html

xi) "Aadhaar covers 99% of adults in India: Prasad", the Hindu, 27 January, 2017, viewed 21 February, 2017 from http://www.thehindu.com/business/Aadhaar-covers-99-of-adults-in-India-Prasad/article17104609.ece

xii) Banerjee, S. 2015, Aadhaar: Digital Inclusion and Public Services in India, Background Paper prepared for the World Development Report- 2016 on Digital Dividends.

xiii) "eSign- Online Electronic Signature Service", Controller of Certifying Authorities, Ministry of Electronics and Information Technology, viewed 27st February, 2018 from http://www.cca.gov.in/cca/?q=eSign.html#content-body

xiv) "The Electronic Signature or Electronic Authentication Technique and Procedure Rules, 2015", Published in the Gazette of India, Dept. of Electronics and Information Technology, MEITY, Govt. of India.

xv) 'List of Empanelled e-sign Service Providers", as registered with the Controller of Certifying Authorities, viewed on 3rd march 2018 from http://www.cag.gov.in/cca/?=service-providers.html

xvi) "Aadhaar data leaked: Perils of discounting cyber security", Editorial, The Tribune, 6th January, 2018 viewed on 5th March, 2018 from http://www.tribuneindia.com/news/editorials/aadhaar-data-leaked/524097.html

xvii) Data protection legislation is best bet for Aadhaar security, say experts", The Business Standard, 15 January, 2018, viewed on 7 April, 2018 from http://www.business-standard.com/article/opinion/data-protection-legislation-is-best-bet-for-aadhaar-security-**say-experts-118011500023_1.html**

Quiz

Try this Out

1. Why would a hacker use a proxy server?

- **A.** To create a stronger connection with the target.
- **B.** To create a ghost server on the network.
- **C.** To obtain a remote access connection.
- **D.** To hide malicious activity on the network.

2. Which of the following is not a factor in securing the environment against an attack on security?

- **A.** The education of the attacker
- **B.** The system configuration
- **C.** The network architecture
- **D.** The business strategy of the company
- **E.** The level of access provided to employees

3. To hide information inside a picture, what technology is used?

- **A.** Rootkits
- **B.** Bitmapping
- **C.** Steganography
- **D.** Image Rendering

4. Which phase of hacking performs actual attack on a network or system?

- **A.** Reconnaissance
- **B.** Maintaining Access
- **C.** Scanning
- **D.** Gaining Access

5. Attempting to gain access to a network using an employee's credentials is called the _____ mode of ethical hacking.

- **A.** Local networking
- **B.** Social engineering
- **C.** Physical entry
- **D.** Remote networking

6. Which of the following is not a typical characteristic of an ethical hacker?

- **A.** Excellent knowledge of Windows.
- **B.** Understands the process of exploiting network vulnerabilities.
- **C.** Patience, persistence and perseverance.
- **D.** Has the highest level of security for the organization.

7. What is the purpose of a Denial of Service attack?

- **A.** Exploit a weakness in the TCP/IP stack
- **B.** To execute a Trojan on a system
- **C.** To overload a system so it is no longer operational
- **D.** To shutdown services by turning them off

8. The first phase of hacking an IT system is compromise of which foundation of security?

- **A.** Availability
- **B.** Confidentiality
- **C.** Integrity
- **D.** Authentication

9. A ------- is a computer program that can invade computer and perform a variety of functions ranging from annoying (e.g. popping up messages as a joke) to dangerous (e.g. deleting files or destroying your hard disk).

A. MS Word
B. MS Access
C. Antivirus
D. Computer Virus

10. When a logic bomb is activated by a time related event, it is known as -------

A. virus
B. Trojan horse
C. time related bomb sequence
D. time bomb

11. The altering of data so that it is not usable unless the changes are undone is

A. ergonomics
B. compression
C. biometrics
D. encryption

12. To protect yourself from computer hacker, you should turn on a _____.

A. Script
B. Firewall
C. VLC
D. Antivirus

13. VIRUS stands for

A. Very Intelligent Result Until Source
B. Very Interchanged Resource Under Search
C. Vital Information Resource Under Seize
D. Viral Important Record User Searched

14. The first computer virus is --------

A. I Love You
B. Blaster
C. Sasser
D. Creeper

15. A _____ is anything that can cause harm.

A) Vulnerability
B) Phish
C) Threat
D) Spoof

**Answers will be provided in the next issue. However we request you to send your answers to aaoita2@cag.gov.in

Learn a term

Block Cipher

A block cipher is a symmetric cryptographic algorithm that operates on a fixed-size block of data using a shared, secret key. Plaintext is used during the encryption, and the resulting encrypted text is called a ciphertext. The same key is used for both the encryption of the plaintext and the decryption of the ciphertext

Countering IT Threats with open source Firewall & Thin Clients

Compiled by: Ajay Shukla, Assistant Audit Officer

Profile of Author

Ajay Shukla works as an Assistant Audit Officer in the "Information Technology Management Group" of the Office of the Principal Director of Audit (Central), Ahmedabad.

Till recently, like many others, cyber security issues never bothered me until one day one of my friend called me over phone and informed that one of his servers was taken hostage by a ransomware. He asked me to resolve the issue, however, the only alternative left was to restore the backups. This incident was indeed an eye opener.

Similar to the real world, the virtual world of internet, otherwise called the cyber space, is filled with vulnerabilities and threats. Insecure and unchecked access to internet can prove disastrous to an organization. Analogous to real world, trusting strangers in virtual world may bring havoc.

Table: Commonly noticed threats in the cyber space

Sl. No.	Types of Threats	Nature of threats
1.	Botnets	Botnets are software robots that create an array of infested computers that are remotely controlled by the Botnet creator.
2.	Distributed denial-of-service (DDoS) attack	A distributed denial-of-service (DDoS) attack occurs when a rogue user deploys a network of zombie computers to disrupt a specific website or server.
3.	Malware	Malwares are malicious software that infects your computer. Computer viruses, worms, Trojan horses, spyware, and adware are classified as malwares
4.	Ransomware	Ransomware is a type of malware that restricts access to your computer or your files and demands ransom for the restriction to be removed.
5.	Spyware	Spyware and adware software collect personal information present in a system without knowledge of its users

The IT threats (See Table) and risks arising out of them in the cyber space, can be mitigated by the following steps:

1. Putting a Unified Threat Management (UTM) system, in place.
2. Installation of software based perimeter to stop any malware that get through the UTM
3. Follow good security practices. Avoid opening email attachments, especially if they are from unknown people.
4. Using thin clients

What is Unified Threat Management?

Unified Threat Management (UTM) devices are hardware network appliances that combine firewalls along with other security features such as anti-phishing, anti-spam, packet inspection, anti-virus etc.

What is a Firewall?

A firewall is a network security device. It monitors incoming and outgoing network traffic. It uses predefined rules to control incoming and outgoing network traffic. A firewall acts as a barrier between trusted and untrusted networks. Firewalls are most basic type of network security function. Actually Unified Threat Management (UTM) devices are enhanced form of firewalls that incorporate other essential security features.

What a firewall (or UTM) can do for us?

Rogue and unscrupulous websites pick up their prey by offering free software, movies and songs as bait. Visitors to these sites unconsciously download ransomwares and malwares which in course of time infect the computers and servers attached to the network. Using a Firewall, one can deny access to rogue sites, curbing the problem. Firewalls can thus prevent cyber-attacks by

- Restricting users from accessing unwanted websites. This can prevent harmful contents, malwares, ransomware etc. from entering the network.
- Defining rule for accessing websites and web applications.
- MAC Filtering, it can block other mobile devices or laptops from accessing one's network
- Managing bandwidth limit, surfing quota limit
- Categorising users in different roles for better user management.
- Creating a captive portal for controlled internet access. Only authorized users can access the internet or any specified part of the network.
- Generating report for accessed websites and data usage.
- Acting as a Dynamic Host Configuration Protocol (DHCP) server, Domain Name System (DNS) server, router and other application-specific network appliances.

Open Source Firewalls

Firewall may either be Hardware Based or Software Based. Further, not many of us know that there are both propriety and Open source **Firewalls available**.

Advantages and Disadvantages of Open source firewalls

Open source firewalls are free to install and source code is available freely which can be customized as per requirement of organizations. On the other hand, Propriety firewalls are priced, expensive and require frequent pricey license renewals on an annual basis. Where availability of financial resources is a constraint, open source firewalls come to the rescue of System Administrators.

Support services are not available free of cost or have to rely on corresponding community.

Some Open Source firewall software

PfSense and Opnsense are two popular open source firewalls that can be harnessed as UTM firewall. Both firewalls are open source operating systems, used to turn a computer into a firewall or router.

A firewall can be assembled by installing PfSense or Opnsense on a commodity computer having at least two network interface cards (NICs).

Pfsense :-

PfSense is considered for its reliability and it offers many features which are mostly found in commercial firewalls. Many third party free software plugins can be integrated in PfSense for extra functionality.

Followings are most popular third party plugins: -

a. ClamAV Antivirus.
b. Iftop: a real time interface monitor.
c. Nmap: A network exploration and security manager.
d. Squidguard: used for webfiltering.

Together with plugins and appropriate hardware, pfsense can be deployed as a UTM (Universal Threat Management).

PfSense provides an easy way to set up a captive portal for your network. Using the portal allows

directing the users on one's network to a specific web page before they are allowed to access the internet. The web page requires a username and password for authentication.

Most commonly PfSense is deployed as a perimeter firewall, with an Internet connection plugged into the WAN side, and the internal network on the LAN side.

PfSense has a customized operating system specifically designed for use as a firewall and/or as a router. PfSense is a customized FreeBSD distribution. Specifications of required hardware depends on the required features to be used and required throughput.

A firewall requires a minimum of two NICs to function properly, one for internal traffic (LAN) and one for external traffic (WAN). Separate Network Interface Card (NIC) is required for every interface of the firewall(computer). This establishes a physical segregation of network traffic.

PfSense can be downloaded from
https://www.PfSense.org/download/

Opnsense

Opnsense is a free firewall and routing platform. It contains most of the features available in high end commercial firewalls. It has a sleek graphical interface. The Opnsense project is a fork of PfSense.

Opnsense can be downloaded from
https://Opnsense.org/download/

Achieving security by deploying Thin Clients

What are Thin Clients?

Thin clients are very small low cost computers and often no data is stored locally in these computers. Thin clients do not have any hard disk and are connected to the server. All computation is done on the server and role of the thin client is only to provide a remote access (remote desktop) to the server.

Thin clients provide better alternative to traditional computers. Apart from cost reduction and better manageability, thin clients provide better security features.

Though Thin clients do not directly contribute to security, however, implementation of the same in an organization gives more control to the administrator thus contributing to enhanced security. Thin clients can be managed and monitored from a single central point.

Software control in thin clients

One of the ways to prevent entry of malicious software is that the IT administrators should not permit users to install unauthorized software, especially software of unknown origin. Applications downloaded from Web sites often contain Trojans and other malicious code that can cause havoc in the systems and leak data. IT Administrators have much greater control over application installations and configuration management in a thin-client architecture.

The Benefits of Thin Client Security Include:

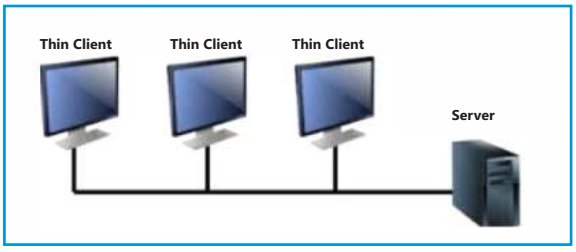


Image : How thin clients works

Thin clients are protected from the use of unauthorized software or the introduction of viruses. Data cannot be copied to a disk or saved to any other location than the server.

Centralized processing makes it easy to manage and monitor the system, simplifies security, protect intellectual property, and ensure data privacy.

Organizations can switch to thin client for achieving more security as well as reduction in capital cost. Thin client devices and solutions are

helping global companies substantially reduce IT security and support costs without compromising on reliability and scalability. The protocols that Thin Clients use to communicate with the server are standard Ethernet, and so don't interfere at all with regular network traffic. In fact, there are many organizations which are replacing PCs with Thin Clients leading to decrease in overall network traffic. At the main server end we install the firewall to reduce the cost of IT support & security.

Learn a Term

Brute Force Attack

A brute force attack is a trial-and-error method used to obtain information such as a user password or personal identification number (PIN). In a brute force attack, automated software is used to generate a large number of consecutive guesses as to the value of the desired data. Brute force attacks may be used by criminals to crack encrypted data, or by security analysts to test an organization's network security.

A brute force attack is also known as brute force cracking or simply brute force.

Hardening

Hardening refers to providing various means of protection in a computer system. Protection is provided in various layers and is often referred to as defense in depth. Protecting in layers means to protect at the host level, the application level, the operating system level, the user level, the physical level and all the sublevels in between. Each level requires a unique method of security.

A hardened computer system is a more secure computer system.

Hardening is also known as system hardening.

Parasite Hosting

Parasite hosting is a search engine optimization (SEO) technique that involves posting a free blog, wiki or forum on a highly respected domain with a high page rank. These free posts are used to create backlinks to a given site, which may boost that site's search engine page rank, thanks to the host's high rank.

Parasite hosting may also refer to hosting a Web page on someone else's server without the latter's permission and then reaping the benefits of the latter's high search engine rank. This trick is often conducted on sites with a ".edu" top-level domain, which search engines such as Google rate as having high authority.

Parasite hosting may also be known as parasitic hosting.

Web Application Security – Issues and Challenges

Compiled by: Sangita Choure,
Pr. Accountant General (Audit-I), Maharashtra, Mumbai
Ravikiran Ubale, Dy. Accountant General
Raghoothaman EPV, Sr. Audit Officer

Profile of Author

Ms. Sangita Choure, IAAS is B.COM, LLM with Diploma in Financial Management from University of Mumbai. She is 1987 Batch Indian Audit and Accounts Service (IAAS) Officer and presently posted as Principal Accountant General (Audit) I, Maharashtra, Mumbai.

Profile of Author

Shri Ravikiran Ubale, IAAS is 2010 Batch Indian Audit and Accounts Service(IAAS) Officer. Presently posted as Deputy Accountant General (SS-I), Office of the Principal Accountant General(Audit)-I, Maharashtra, Mumbai. He is a trained trainer of Data Analytics and he has delivered lectures on various other topics like PPP Audits, IT Audits, E-Governance, ISSAI's.

Introduction

Majority of Government departments are now using web-based applications for improving government efficiency and transparency in delivery of various citizen services like tax, treasury, procurement, vehicle registration, licenses, railway booking and Aadhaar etc. The Union and many State Governments are also giving thrust to implement various welfare schemes through Direct Benefit Transfer (DBT), program to transfer benefits/subsidies directly to the people through their bank accounts such as scholarships, gas subsidies, wages, housing subsidies and subsidies to farmers.

Although the Web applications, through which the services are delivered, increases the efficiency of the Government, they interact with database systems storing sensitive and critical information, thereby bringing a set of vulnerabilities, risks and Security threats posing challenges to the smooth operation of an organization.

In the recent times, we have witnessed security breaches of web applications like the scholarship disbursal scam in one district of Maharashtra and misuse of Aadhaar data for unauthorised diversion welfare funds (mainly LPG subsidies) by telecom companies. These incidents demonstrate the vulnerabilities in the systems relating to DBT. This highlights the need for serious thinking on web security so as to avoid and prevent damage to the information assets.

A web application is any programe that runs in web browser, typically created in a browser – supported programming language and relies on web browser to render the application. Typically, attackers attacks or exploits vulnerabilities in the application. A software "vulnerability" is an unintended flaw or weakness in the software that leads it to process critical data in an insecure way. By exploiting these "holes" in applications, cybercriminals can gain entry into an organization's systems and cause damage to the information assets like confidential data.

Attackers can potentially use many different paths through the application to inflict damage to any business or organization. Each of these paths represents a risk that warrants our attention.

Web Security Standards

As far as international web security standards are concerned, the Open Web Application Security Project (OWASP) is an open-source application security community whose goal is to spread awareness surrounding the security of applications. This organisation publishes a list of what it considers the current top 10 web application security risks worldwide, known as OWASP Top 10 (See Table I), every three/four years prioritizing the top 10 according to their prevalence and their relative exploitability, detectability, and impact. Because the risks to applications are always evolving, the OWASP Top 10 list is revised each time to reflect these changes, along with the techniques and best practices for avoiding and remediating the

vulnerabilities. These top 10 vulnerabilities can be used as a point of reference in any security audit relating to web application.

In the Indian scenario, in the year 2011, Standardisation Testing and Quality Certification (STQC), Directorate, Ministry of Communication and Information Technology, GOI also issued Guidelines for compliance to Quality requirements covering Security and Transparency. These guidelines and standards help determine the focus areas in a Web Application Security Audit.

Table I: OWASP Top 10 2017

Risk	How it Works	Impact
1. Injection of queries	Injection flaws, such as SQL injection, refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server	Injection can result in data loss, corruption, or disclosure to unauthorized parties, loss of accountability, or denial of access. Injection can sometimes lead to complete host takeover.
2 Broken Authentication	Application functions related to authentication and session management are often implemented incorrectly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities temporarily or permanently.	Attackers have to gain access to only a few accounts, or just one admin account to compromise the system which may result in money laundering, social security fraud, and identity theft, or disclosure of legally protected highly sensitive information.
3 Sensitive Data Exposure	Sensitive data may be compromised without extra protection, such as encryption at rest or in transit, and requires special precautions when exchanged with the browser.	Failure frequently compromises all data that should have been protected. Typically, this information includes sensitive personal information data such as health records, credentials, personal data, and credit cards, which often require protection as defined by laws or regulations or local privacy laws.
4. XML External Entities (XXE)	Many older or poorly configured XML processors evaluate external entity references within XML documents. External entities can be used to disclose internal files using the file URI handler, internal file shares, internal port scanning, remote code execution, and denial of service attacks.	These flaws can be used to extract data, execute a remote request from the server, scan internal systems, perform a denial-of-service attack, as well as execute other attacks.
5 Broken Access Control	Access control is meant to control what "authorized" users are allowed and not allowed to do within an application. A flawed access control may be caused by unenforced user restrictions and this allows attackers to exploit and access unauthorized functionality or data.	The technical impact is attackers acting as users or administrators, or users using privileged functions, or creating, accessing, updating or deleting every record.
6 Security Misconfiguration	Security Mis-configuration arises when Security settings are defined, implemented, and maintained as defaults. Good security requires a secure configuration defined and deployed for the application, web server, database server, and platform. It is equally important to have the software up to date.	Such flaws frequently give attackers unauthorized access to some system data or functionality. Occasionally, such flaws result in a complete system compromise.
7 Cross-Site Scripting (XSS)	XSS flaws occur whenever an application includes un-trusted data in a new web page without proper validation or escaping, or updates an existing web page with user-supplied data using a browser API that can create HTML or JavaScript. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.	The impact of XSS is remote code execution on the victim's browser, such as stealing credentials, sessions, or delivering malware to the victim.
8 Insecure Deserialization	Insecure Deserialization is a vulnerability which occurs when untrusted data is used to abuse the logic of an application, inflict a denial of service (DoS) attack, or even execute arbitrary code upon it being deserialized.	The impact of deserialization flaws cannot be understated. These flaws can lead to remote code execution attacks, one of the most serious attacks possible.
9 Using Components with Known Vulnerabilities	Applications and APIs using components with known vulnerabilities may undermine application defences and enable various attacks and impacts. There are automated tools to help attackers find unpatched or misconfigured systems.	While some known vulnerabilities lead to only minor impacts, some of the largest breaches to date have relied on exploiting known vulnerabilities in components.
10 Insufficient Logging & Monitoring	Insufficient logging and monitoring vulnerability occurs when the security-critical events aren't logged properly, and the system is not monitoring the current happenings	Most successful attacks start with vulnerability probing. Allowing such probes to continue can raise the likelihood of successful exploit to nearly 100%. To prevent such attack, establish effective monitoring and alerting such that suspicious activities are detected and responded to in a timely fashion.

Profile of Author

Raghoothaman EPV is a BSc, PG Diploma in Computer Systems and Management. He is a Senior Audit Officer in the Office of the Principal Accountant General (Audit)-I, Maharashtra, Mumbai. He has been involved in the IT Audit of various systems such as e-Tendering System in Government Departments, e-Aushadhi System, Government Receipt Accounting System, Aqua- Water Billing system in Municipal Corporation of Greater Mumbai (MCGM) and Maharashtra Vikrikar Automation System (MAHAVIKAS).

Web security in the Government of Maharashtra

The recent CAG audit of e-Procurement system implemented by the Maharashtra Government (published in 2017) and Property Tax system implemented in the Municipal Corporation of Greater Mumbai indicated that periodic cyber security audit was not conducted on these web applications as required.

Government of Maharashtra (GoM) has formulated a comprehensive e-Governance policy in 2011 to ensure standardized and seamless implementation of e-Governance projects across the State, thereby encouraging interoperability, data collaboration, sharing and linkage with UID. It also covers various aspects of web application security. Various citizen services have been made available online through the State Portal in-line with the National Portal of Government of India and through other channels like Common Service Centres, Setu, CFC, Mobile platforms etc.

GoM policy also states that all websites and Web-based applications are required to comply with Website design guidelines issued from time to time by Government of India and should have proper security certifications. Periodic cyber security audit of all State government websites is also mandatory, and no website or portal or application shall be hosted at the State Data Centre without security audit and compliance.

Web Security Audit strategy

- Identify the risk and categorise the risk as High, Medium, low.
- Verify controls associated with four important risks
    a. **Input validation** – controls such as initial values, error/exception handling, logging, fail safe vs fail open and resource exhaustion controls
    b. **Authorization** – controls such as tokens & Two-Factor Authentication (2FA), authorize transaction, not user, use of Certificates for non-repudiation, Adaptive Authorization, site keys and out of band (SMS/voice)
    c. **Data Protection** – controls such as valid SSL certs, encrypted connection strings, encrypted cookies and encrypted database
    d. **Session Management** – controls such as session time limits, Geo location, IP, known PC and hard to guess session variables/IDs
- Performing the tests – what, who and where
    a. What: what do you have? What data is in the system? And what is the value of the data?
    b. Who: trusted third party developer or ASP, unknown third party developer or ASP, trained and seasoned development team, eager and inexperienced development team and business unit management purchase.
    c. Where: Local Internet Web application, public website hosted internally, customer portal hosted internally, remotely hosted web application and connectivity, firewall, transport, etc.
- OWASP – Testing Guide: WebGoat is a deliberately insecure web application maintained by OWASP designed to teach web application security. Once deployed, the user can go through the lessons and track their progress with the scorecard. There are currently over 30 lessons.

OWASP Testing Guide essentially provides for framework for Security Audit of web application giving in detail various security testing and Audit checklist associated with it, such as Configuration and Deployment Management Testing, Identity Management Testing, Authentication Testing, Authorization Testing, Session Management Testing, Input Validation Testing, Business Logic Testing and Client Side Testing etc. This will help the auditor in assessing the web application security risks and conducting security audit of such systems.

Way Forward

It is needless to say that all web-based applications of the Government Departments and Local Authorities need to comply with e-Governance policy of the Centre and State Governments. IT auditors will have to use international standards and guidelines like OWASP in addition to the national policies in the web security audits to ensure a secure web and cyber space.

REFERENCES:

i) Information Technology Audit of e-Tendering System in Government departments - Principal Accountant General (Audit)-I, Maharashtra – AR on General and Social Sector for the year ended March 2016 (Para – (i) Open Web Application Security Project (OWASP), (ii) Broken Access Control)

ii) STQC Guidelines for compliance to Quality requirements of e-Procurement Systems (Para - Open Web Application Security Project (OWASP).

iii) https://www.owasp.org/index.php/Top_10-2017_Top_10 (Para - OWASP Top 10 2017 Application Security Risks 1 to 10)

iv) e-Governance policy of Government of Maharashtra (Para - e-Governance policy in the Government of Maharashtra)

v) ISACA – IT Audit strategies for web applications (Para – What Auditors should do)

Gadgets Info

eSight 3

In a world of Internet-connected coffee makers and juicers and whatnot, gadget aiming to solve problems of a higher order seems to be an interesting find. The eSight is an over-eye visor that helps legally blind people navigate via a combined high-definition camera and video display. Showing a live feed on a pair of OLED displays placed in front of the wearer's eyes, the lightweight, hands-free device does everything from read to provide directions. With virtually no input lag from the front-facing camera to the screens, eSight is a true augmented reality headset.

Image source: abledata.acl.gov

L'Oreal's

L'Oréal's UV Sense is a tiny sensor capable of detecting ultraviolet exposure that's small enough to wear comfortably on your fingernail. The sensor itself is battery-free and includes an NFC (Near-Field Communication) antenna, a temperature sensor, and a UV sensor.

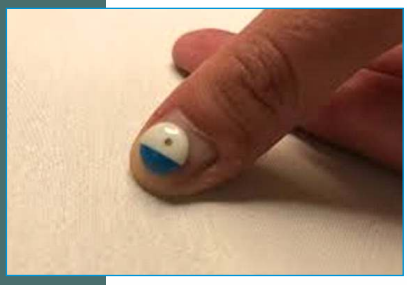


Image source: http://c.mi.com

Update Corner

Updates on Malware/Virus/Worms

This section provides information on latest Malaware/Virus/Worms

1. Zeus/Zbot Trojan

Zeus, ZeuS,or Zbot is Trojanhorse malware package which runs on versions of Microsoft Windows. While it can be used to carry out many malicious and criminal tasks, it is often used to steal banking information by man-in-the-browser keystroke logging and form grabbing. The virus was distributed in an e-mail, and when targeted individuals at businesses and municipalities opened the e-mail, the trojan software installed itself on the victimized computer, secretly capturing passwords, account numbers, and other data used to log into online banking accounts. The hackers then used this information to take over the victims' bank accounts and make unauthorized transfers of thousands of dollars at a time.

2. ATM Jackpot

ATM Jackpot is a new kind of malware, which forces ATMs to spit out huge wads of cash. This malware appears to have originated from Hong Kong and may still be under development, according to California-based software company Netskope. ATM jackpotting by cyber criminals has been taking place for many years now, predominantly in Europe and Asia, and have recently surfaced in the USA too. This software is similar to other ATM malware, such as 'ATM Ripper,' unearthed in 2014, which also forces devices to dispense large amounts of cash. However, unlike similar software, ATM Jackpot has a smaller system footprint and a 'very simple' graphical user interface. To install the malware, thieves often require physical access to the ATM

machines. Hackers only need access to the ATM's motherboard, which is protected by a door and key that's easily opened. From there, they could insert a USB flash drive that contains the malware and the ATM will start freely spitting out some cash. However, it is yet to be known, how ATMJackpot is deployed - to whether the cyber attackers install it physically or remotely.

3. Shortcut virus

Shortcut virus is a virus which finds its way in to the flashdrive, PC, Hard Disk, Memory cards or mobile phone and changes the files into shortcuts with the original folder icons. The risk is that, on clicking on the shortcut icon, there is every chance of the data getting lost and the computer being infected. Shortcut files — or those ending in the ".lnk" extension — are Windows files that link (hence the "lnk" extension) easy-to-recognize icons to specific executable programs, and are typically placed on the user's Desktop or Start Menu. The virus is activated with a click by the user, on the shortcut icon. It has been noticed that these malicious shortcut files are capable of executing automatically if they are written to a USB drive that is later accessed by Windows Explorer.

Here's how to remove the infection from the external device:

1. Plug in the infected external device.
2. Open File Explorer (Windows key + E keyboard shortcut) and look under the Devices and drives section to find the external device, then make a mental note of the drive letter (e.g. E:).
3. Launch an elevated Command Prompt by opening the Power User Menu (Windows key + X keyboard shortcut) and selecting Command Prompt (Admin).
4. Orient the Command Prompt to the external device by typing the drive letter you noted in step 2, then hitting Enter:E:
5. Delete all shortcuts on the device with this command:

   del *.lnk
6. Restore all files and folders on the device with this command:

   attrib -s -r -h /s /d *.*
7. It is now done!

The attrib command is a native Windows function that alters the attributes of a particular file or folder. The other parts of the command designate which files and folders to alter and how they should be altered:

- -s removes the "system file" status from all matching files and folders.
- -r removes the "read-only" status from all matching files and folder.
- -h removes the "hidden" status from all matching files and folders.
- /s makes the command recursively apply to all files and folders in the current directory and all subdirectories, basically the entire device in this case.
- /d makes the command apply to folders as well (normally attrib only handles on files).
- *.* means all file names and folder names should be considered a match.

Once the above is done, consider copying all of the files off of the external device, completely formatting the external device to wipe it clean, then moving the files back onto the external device.

Source Links:-

i) http://www.dailymail.co.uk/sciencetech/article-5596665/Security-researchers-new-form-malware-lets-hackers-hijack-ATMs-spit-money.html

ii) https://www.makeuseof.com/tag/remove-shortcut-virus/

https://funnymemes.co

Update Corner

Hardware

1. **Bluetooth5-** Laptops and 2-in-1s will be equipped with the latest Bluetooth 5 wireless specification, which is a longer and faster upgrade to the ageing Bluetooth 4.2. Bluetooth 5 will allow PCs to communicate wirelessly with devices up to 400 meters away in clear line of sight, but a more reasonable range is about 120 meters, according to analysts. Bluetooth 5 will transfer data at speeds of up to 2Mbps, which is two times faster than its predecessor.
2. **USB Type C**- PC makers may not muster up the courage to remove the headphone jack and SD card slots from PCs right away, but USB 2.0 slots could be on their way out. Some PC makers may leave out display and other legacy ports with the emergence of the versatile USB Type-C, which can be used to charge PCs and connect displays, storage devices and other peripherals.

Latest updates on e Governance projects implemented by Government of India

A Mission Mode Project (MMP) is an individual project within the National e-Governance Plan (NeGP) that focuses on one aspect of electronic governance, such as banking, land records or commercial taxes etc.

Within NeGP, "Mission Mode" implies that projects have clearly defined objectives, scopes, and implementation timelines and milestones, as well as measurable outcomes and service levels.

The NeGP comprises 44 Mission Mode Projects (MMPs), which are further classified as Central, State and Integrated Projects. The theme of the next issue of PursuIT will be on E- Governance. Articles may be sent to aaoita2@cag.gov.in by August 2018The 44 Mission Mode Projects are categorized and divided – 13 Central MMPs, 17 State MMPs and 14 Integrated MMPs. MMPs are owned and spearheaded by various Line Ministries. State Governments are responsible for implementing State MMPs, under the overall guidance of respective Line Ministries in cases where Central Assistance is also required. The Department of Electronics and Information Technology (DeitY) acts as the facilitator and catalyst for the implementation of NeGP and provides technical assistance to various Ministries/Departments and State Governments.

The theme of the next issue of PursuIT will be on E- Governance. Articles may be sent to aaoita2@cag.gov.in by August 2018

Skill Shop

Update your skills, the e-way!!

SWAYAM is a programme initiated by Government of India and designed to achieve the three cardinal principles of Education Policy viz., access, equity and quality. The objective of this effort is to take the best teaching learning resources to all, including the most disadvantaged. SWAYAM seeks to bridge the digital divide for students who have hitherto remained untouched by the digital revolution and have not been able to join the mainstream of the knowledge economy.

This is done through an indigenous developed IT platform that facilitates hosting of all the courses, taught in classrooms from 9th class till post-graduation to be accessed by anyone, anywhere at any time. All the courses are interactive, prepared by the best teachers in the country and are available, free of cost to the residents in India. More than 1,000 specially chosen faculty and teachers from across the Country have participated in preparing these courses.

The courses hosted on SWAYAM are in 4 quadrants – (1) video lecture, (2) specially prepared reading material that can be downloaded/printed (3) self-assessment tests through tests and quizzes and (4) an online discussion forum for clearing the doubts. Steps have been taken to enrich the learning experience by using audio-video and multi-media and state of the art pedagogy / technology.

Take a look at the courses in www.swayam.gov.in, www.nptel.ac.in. An indicative list of free or nominally charged courses on IT, useful to auditors are given in the table below:

	Title of the Course/Link to the website
	Introduction to Computers and IT Concepts
	https://www.udemy.com/fundamental-computer-information-technology-video-lectures/
	Introduction to computer Hardware/Software and their troubleshooting
	https://www.udemy.com/computer-cavalry-intro-pc-maintenance-rocket-science-1/
	M S Office
	https://www.udemy.com/fundamental_computing_skills/
	Database concepts, System concepts
	http://nptel.ac.in/courses/106104135/
	Oracle with SQL Queries
	https://www.udemy.com/introduction-to-databases-and-sql-querying/
	CAAT-SQL
	https://www.udemy.com/introduction-to-databases-and-sql-querying/
	Linux
	https://www.udemy.com/introduction-to-linux-centos-7/
	Window Server
	https://www.udemy.com/windows-server-2012-for-beginners/
	Networking Concepts & Internet
	http://nptel.ac.in/courses/106105081/
	http://nptel.ac.in/courses/106105080/
	http://nptel.ac.in/courses/106106091/
	IT Security issues- Network Security & Assessment
	https://www.udemy.com/network-security-essentials-novodyne/
	IT Security & Cyber Law
	https://www.udemy.com/cyber-security-law/
	Information System Security Management
	https://swayam.gov.in/courses/1303-introduction-to-information-security-i
	Cloud Computing
	https://swayam.gov.in/courses/4413-cloud-computing
	Crypto Currencies/Bitcoins
	https://www.gcflearnfree.org/computerbasics
	Mobile Computing
	http://nptel.ac.in/courses/106106147

Disclaimer

This Journal is conceived, designed and presented by International Centre for Information Systems and Audit (iCISA) which is a field Office of SAI, India, for internal circulation within Indian Audit and Accounts Department only.

This Journal aims to share with readers the latest developments in the field of Information Technology and shall be used for information ONLY. Though all efforts have been made to ensure the accuracy of the facts and figures, the same shall not be construed as statement of law or used for any legal purposes. In case of any ambiguity or doubts users are advised to check it with the authors and officers of iCISA before taking any decision based on information contained therein. The contents of this journal are meant for informational purposes only. iCISA disclaims all liability for actions taken or failed to be taken based on any content of this journal.

This Journal has provided web links to various outside websites also for information ONLY and hence does not assume any responsibility for the contents included therein.