International Journal of Electrical Electronics & Computer Science Engineering
Special Issue - TeLMISR 2015, ISSN : 2348-2273
Available Online at www.ijeecse.com

Digital Security: A Moving Target

Avijit Dutta, Scientist 'F'
National Informatics Centre, A Block CGO Complex, Lodhi Road, New Delhi, India
dutta_avijit@yahoo.com

Abstract: ***Advances in technologies and their integration open up new horizon of knowledge and elevates society to a higher level of unknowns and ignorance. New questions replace answered ones and quest for superior realization continues with associated risks and pitfalls. Progresses in technology and emergence of standards to measure, evaluate and integrate them addressed many complex problems easing human life. This continued across technology evolution stages like agrarian, semi-industrialisation, advanced industrialisation and Information age [1, 2, 3, 4, 5]. Path breaking insightful innovations, during these ages, made deep inroads into life processes and with growing usages got glued inseparably with it as Mark Weiser talked about profound technologies in his seminal paper in Scientific American titled "The Computer for the 21st Century" [18, 19].***

In this process, power shifted from Agrarian to Steel and then to Information and Communication Technology (ICT). ICT has now become tool for dominance. It has inducted pace in daily activities and concept integration, allowing flexibility in process management that affects life, albeit raising new threat perception.

Technology Innovation and Integration (TII) on fast track has transformed the concept of wealth from tangible to intangible objects, from material to intellectual aspect. One needs to accept that TII opens up avenues for both productive and destructive collaborations. It is well known that while speed thrills, it kills too. In this age of ubiquitous computing, security threats goes beyond closed doors as digital objects now can exchange pervasive signals through touchable, solid mediums raising fear for loosing intellectual and material wealth along with physical wellness. Present text attempts to create a window view of advances in technology, technology integration, ICT and emerging security perception associated with it [7, 8, 9, 11].

Keywords: Information and Communication Technology, Internet, Internet of Things (IoT), Pervasive Healthcare, Pervasive Healthcare Systems, Technology Innovation and Integration.

I. INTRODUCTION

The history of mankind is on a fast track. Our planet came to existence approximately for four billion years though all known species on it came to existence roughly less than a hundred million year ago and existence of human being are only one million year narrative. The printing press started dissemination of knowledge from around second century and invention of steam engine, which tossed us to industrial age, happened only in 1712. Innovation and concept integration from different fields of mathematics, natural sciences, technology, philosophy etc. added new dimensions to the process of novelty. Today's ICT evolved out of such process where innovations form many areas joined hands to usher a new realm of science involving Computer, Communication and its Applications.

Society marched ahead to add wealth to physical and intellectual possessions [2, 3, 4, 5] to alter security perception as fear of losing the possession grew with affluences. At this juncture one may not lose the sight of the fact that the act of stealing offers tremendous incentives in terms of gain in time and capital. It is accepted as one of the areas of art from ancient period, which thrived over time and used by both legal and illegal agencies all across the world forcing continuous discovery of new defense techniques against it. If the act gets into one's pathological system the sense for righteousness goes for a toss. Incidents are in abundance where entire community and country gets involved in the so called sinful process. Just by stealing 'Identity Code' or a 'Password' one can gain access to a fortune that took years to accumulate. Hacking, Cracking etc. are intellectual exercises now which are at times used over Internet by entities on either side of the legal line of a country.

Technology follows uniform standards all across the globe. However, technology management processes and legality associated with it follows different approaches at different part of the world. ICT with its today's strength allows one to hack or breach access right of an Internet segment from one corner of world considering it illegal and seek shelter elsewhere in the globe where same act stands acceptable. Examples supporting the fact are many.

One need to be scared as hacking is part of academic curriculum in many institutions in the country and abroad and so are the concepts of defenses like data hiding, embedding and protecting. Cryptography is one such areas of act for data protection and hiding, which follows defined standard and practices, but exceptions are many either. In this backdrop security issues of digital wealth is discussed and in the journey, evolving aspects of Digital Computing and Communicating Technology and their usage patterns are touched upon for better insight.

II. DIGITAL COMPUTING

First generation of modern computers of industrial era evolved during 1947-49. The evolution of computers and computing techniques continued through second, third and fourth generation of present age and still

International Journal of Electrical Electronics & Computer Science Engineering
Special Issue - TeLMISR 2015, ISSN : 2348-2273
Available Online at www.ijeecse.com

moving ahead to autonomic computing of fifth generation [6] at a sky-high pace making earlier generations appear archaic quickly [2,3,4,5]. Over year's digital computing, communicating hardware, software and associated processing and rendering techniques integrated under a banner 'Computing System (CS)', which enhanced capabilities collectively. This allowed other important areas like engineering, physics, mathematics, natural sciences, business processes, commerce, medical science, etc., and their cross sectional areas to take advantage of digital computing capabilities of CS. Languages facilitating application of computers too progressed from first to second, third and fourth generations giving rise to various programming standards like non-procedural, procedural, and object oriented techniques to accommodate more complexity of real life scenario. As time went ahead expanding problem domain evolved demand for component-based solutions with flexibility and reusability of resolution mechanism. This brought in the era of object oriented design (OOD) and development. Digital Communication joined hand with Information Technology (IT) to advance it to ICT (Information and Communication Technology) paradigm. As computing became a common place need, call for digital communication consolidated since both would have ushered realm of ubiquitous computing, visualized by Mark Weiser during nineties of previous century [18,19]. This text thus owes a few words for digital communication too which is presented in next segment.

III. DIGITAL COMMUNICATION

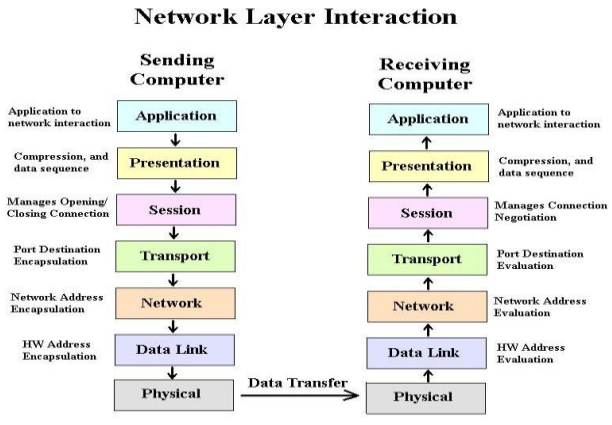

Figure 1

Transmission Control Protocol (TCP) and Internet Protocol (IP), as the protocol suite, commonly known as TCP/IP, emerged as the protocol for ARPANET (Advanced Research Projects Agency Network) packet switching network technology during 1982-83, paving way for digital data sharing to come over age of serial communication through RS-232 links to packet switch networking technology. Establishment of OSI (Open System Interconnection) model (ISO/IEC 7498-1) and TCP/IP model ushered us to INTERNET era, which in fact frames its backbone. In Fig-1 precisely the process of data exchange between two computer systems, in terms of sending and receiving is shown in Seven-layer OSI communication model. This perfectly showcases application of object oriented design (OOD), in technologies integration, following established standards, for successful digital communication.

Technical functioning and system evolution at each layer is independent of other though core objective of live and successful interaction with bordering layers remains intact. All seven layers work seamlessly to make digital packet exchange between two computing systems a success. However, with reference to present context it can be conceived that security threats at each layer would be different and when different layers starts functioning in conjunction, overall security threats simply gets summed up and presents a complex collective scenario. Attackers can target attack to a particular layer or all at a time, difficult though, and disrupt overall functioning. Various digital connectivity options available today like, satellite, terrestrial, R/F, Blue-tooth etc makes vulnerability situation even more complex. A window view of possible security threats at each layer and associated solution is presented in table – 1 below

Table 1: Depiction of Layer wise Security threats in OSI Model

Layer	Security Threat	Solution
Application	Static Password, SNMP Private Community Strings	Anti Virus software, OS Hardening, Patching
Presentation	Viruses, Worm	Intrusion Detection, Auditing
Session	Personal Information Retrieval, Root Privilege Access, Net Bios, DOS	Patches, Encryption, Authentication
Transport	Endpoint Identity	Firewall access control list
Network	Preventing unauthorised access to internal system	VPN network based intrusion detection and content filtering
DATA	ARP spoof, MAC Flooding	Private VLANs, Static ARP (address resolution protocol) entries, STP (Spanning Tree Protocol) root priority
Physical	Inadequate Power, Unfettered access, Open wall ports	Managed Power through UPS, Restricted Access, Close down open wall ports

TCP/IP (Transmission Control Protocol / Internet Protocol): a more precise form of OSI model as depicted in Fig-2 consists of only four layers where in

Application, Presentation and Session is merged in 'Application' layer, Network becomes Internet and Data Link and Physical makes Network Interface Layer, thereby reducing seven layer OSI model to four layer TCP/IP model. In TCP/IP, (TCP) is one of the original components at the core of the Internet protocol suite complementing the Internet Protocol (IP), and the entire suite is known as TCP/IP.

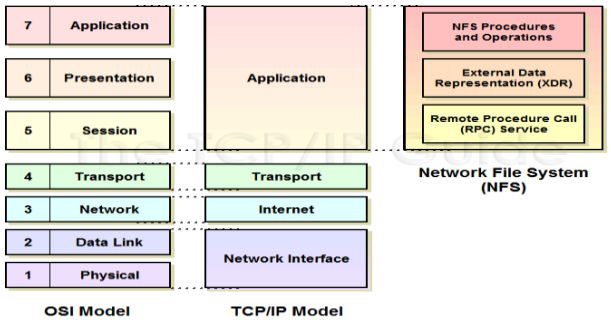

Figure 2

It is important to note that TCP protocol suite used by major Internet applications such as WWW (World Wide Web), HTTP (Hypertext Transfer Protocol - the underlying protocol used by the World Wide Web to define how messages are formatted and transmitted), SMTP (Simple Mail Transfer Protocol - an Internet standard for electronic mail (e-mail) transmission), TELNET (a network protocol used on the Internet or local area networks to provide a bi-directional interactive text-oriented communication facility using a virtual terminal connection) and FTP (File Transfer Protocol - is a standard network protocol used to transfer of computer files from one host to another host over a TCP-based network, such as the Internet. FTP is built on client-server architecture and uses separate control and data connections between the client and the server).

TCP is used for peer-to-peer file sharing and some streaming media applications. It is optimised for accurate delivery rather than timely delivery. For real time applications protocols like Real Time Transfer Protocol (RTP) over User Datagram Protocol (UDP) are generally preferred. Applications, which do not require reliable data stream, may use User Datagram Protocol (UDP). UDP provides a datagram service that calls for reduced latency over reliability. These protocols provide platforms for exchange of data, information and knowledge of today's order. It is essential to note that these applications functions on different ports with varied range of security vulnerability [20].

Computing and communicating together revolutionised the way information were once stored, retrieved and disseminated. The human computer relationship also shifted from one machine - many user of first generation to one machine - one user of second generation to one user - many machine of third generation and then to many machine - many user of fourth generation of present [4,5,12,13]. The paradigm shift took us from serial connectivity to packet switch based LAN (Local Area Network) and to WAN (Wide Area Network) connectivity and to INTERNET, gifting us experience of Web1 and Web2, which evolved over INTERNET. Technology evolution and integration (TII) brought Information and Communication Technology (ICT) at the doorstep of commoners with multiplicity of connectivity, processing and rendering options. However these also raises security concerns like "Who is on the other side of the wire!", "What is getting downloaded or processed on my system!", "Am I hooked on to the right server!" and many more like these. Technology Integration has offered different perspective of the forth-coming circumstances, which calls for due attention [3, 4, 5].

IV. TECHNOLOGY CONVERGENCE

In a different perspective it can be opined that computing has evolved with astronomical pace from standalone monolithic ENIAC system to age of Main Frame Systems, to Personal Computing (PC) System, to Nomadic Computing and then on to Ubiquitous and Pervasive Computing concept of present age**.** L. Kleinrock, in the context of nomadic computing observed telecommunication technology influenced major shifts in the application of communications to satiate the needs of our society and industry. The process led to marriage of technologies like wire line and wireless technologies, analog and digital technologies, technologies of voice, data, video, image, fax, graphics, etc. In entirety this created a computer communications infrastructure that serves billions of people all across the globe. This led us to the midst of an accelerating groundswell in the field of computer communications in its largest sense [4, 6, 7, 10, 18]. This is inclusive of computing system, network systems, associated infrastructure, the middleware, the applications and finally, the uses and users of the technology! To add more, miniaturization of devices, efficacy of network communication and evolution of standards fructified the dream of collective intelligence and agile interaction on virtual plane [3, 5, 12, 13].

Mark Weiser at PARC XEROX accredited as the father of ubiquitous computing, visualised it in his seminal paper titled "The Computer for the 21st Century" in Scientific American that most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it. In essence he visualized an environment saturated with computing and communicating capabilities, which gracefully integrated with human users. The concept now also called pervasive computing. In actuality this perspective paints

a future where in computing system gets embedded and possibly diluted into every conceivable object of our surroundings, replacing visible personal computers, to be indivisible part of day-to-day systems and practices [10, 18, 19].

V. COLLECTIVE RISK

Computing and communicating technology joined hands for Hyper Text Transfer protocol (HTTP) to usher World Wide Web, leading to Web1 era. Web1 allowed us to see information across the world in static form. This could not keep individual interested for long. To keep people glued with it many dynamic features in form of audio, Video and Text with backend database support joined in to bring in Web 2.0 era [5, 16]. These facts apart Web2 allows user to participate in the act of digital show to keep their interest on. Today digital exchange is extending horizons to accommodate more and more individuals to send, receive and evolve data, information and knowledge, leading to wisdom and awareness, using devices and sensors of various forms generally termed as Internet of Things (IoT). Web2 allows individuals to interact with INTERNET in all possible forms like reading and editing stored contents and feeding new information. It has provided a platform for online, real-time mass interactions. Today information in all form is being fed to web not only by simple keyboard interaction of a client system but also with cameras and sensors of different types [16].

The process is evolving a shadow of audio, video and text information with GPS precision over INTERNET. This is, in a way an animating process of INTERNET, which is in a state of increasing sensual maturity. This is like a child, endowed with all senses though void of analytical ability, grows to complete manhood having skills to effectively use senses with passing time as visualised by Tim Orilley. Mr. Orilley talked about collective intelligence of INTERNET, which is being growingly enriched by its users located all across the globe. This collective intelligence enhances community knowledge and can be used to augment quality of life in many forms. However, Mr. Orilley does not miss the sight of the possibility for loosing privacy as number and types of players over the platform increases. As sensors collects location specific data from all around the globe, which is being stored and retrieved at ease by one and all for both known and unknown reasons, a dig into personal, social and intellectual life with trivial causes can not be mistreated [15, 16, 17,18].

INTERNET is altering way of life and its quality touching its every aspect like academics, science, technology, finance, entertainment, arts, culture, social works, professional act, business, future plans and even us with added efficiency though associated risk comes as a pinch of salt, which if goes beyond control blights the entire feast. As size of participants over INTERNET grows, increasingly it is getting difficult to identify the one on the other side of the wire and the activity the entity is interested in who is requesting for a contact or interaction. The risks indicated in table -1 and more associated eventually comes into play. A harmful contact/interaction can cause long-term damage to tangible and intangible assets including health!!! Though one cannot refuse to be on INTERNET now, casual usage of this razor sharp and swift resource can be life threatening as it has come to the notice of Department Of Homeland Security in USA.

Krishna Venkatasubramanian and Sandeep K.S. Gupta [9, 16, 18, 19] talked about Pervasive Healthcare Systems (PHS), which is to change traditional approach that involves visiting a doctor, examinations of symptoms, going through advised medical test and availing treatment. The goal of pervasive healthcare (PH) is to use pervasive computing technologies to provide round-the-clock healthcare outside the confines of traditional medical establishments, such as hospitals and medical clinics but at patient's homes and even outdoors. It is observed that advances in digital communication and sensing technologies has led to the development of intelligent handheld, implantable and wearable devices (such as PDAs, cell phones, smart watches etc.) that have made it possible to implement a wide range of solutions for PH systems. This is to increase the modalities and spatiotemporal dimensions in which healthcare services can be provided for improving patient care outcomes. Author indicates that security is very important in pervasive healthcare systems to protect sensitive health information that is being collected and managed. In this context maintenance of data confidentiality and integrity is essential needing strong authentication features, which controls unauthorized access of personal health information.

PHS is expected to advance Mobile Telemedicine to treat patient from distance, Disaster Response in case of less number of doctors in comparison to number of patient's and Lifestyle Management systems. Quite interestingly Krishna Venkatasubramanian and Sandeep K.S. Gupta advocates the use of the human body itself as a means of generating cryptographic keys (for symmetric cryptography, as Public Key Infrastructure may be too expensive in this context) for securing inter-sensor communication. As the human body presents an extremely dynamic environment, it can produce many specific physiological values that are time-variant and random and are generated from a large range of values which are not easy to guess.

In case of PHS both the sender and receiver can measure the physiological values from their environment and use them for security purposes, when they want to communicate. The principal idea behind this scheme is to ensure privacy of senders and receiver

[9, 18]. From preceding deliberations it can be conceived that security is a perception and it has many dimensions. The thoughts of ubiquitous and pervasive computing as conceived by Mark Weiser are gradually shaping up in actuality. This is further detailed by Tim Orilley leading to the contemplation that a virtual world is getting evolved as an image of real world out there and INTERNET, which was just a kid during previous century, is growing to maturity with all sharpening senses provided by innumerable computers, cameras, and electronic sensors around the world. This process also may produce threats of different form. Thus the worry to loose physical and material wealth to digital attacks are growing and getting real. The possible sources for attacks are also adding dimensions with every passing day. It has been indicated earlier that in this age of ubiquitous computing, security threats goes beyond closed doors as digital objects can exchange pervasive signals through tangible objects and one may expect even physical loss if carrying implantable and wearable devices beyond loss of intellectual and material possessions [15, 16,17,18,19].

VI. DEFENSE

The discussions preceded indicate that sources and nature of digital threats are many. Individual and institutions should attempt to evolve a threat model to plan protection. Most of the threats arise out of unknown or dubious sources. In that sense Identification, Authentication and Authorization of information sources are essential. This can be availed from PKI establishment, where in a Certifying Authority (CA) provides Digital Signature Certificate (DSC) on Public Key of an entity (Individual, Institution, Computer Server etc.) in an asymmetric cryptographic system supported by defined architecture and extensions. In the stated system Controller of Certifying Authority (CCA) administers overall practices of CA, first with a license and key pair to initiate business and then with, directives on policies and practices from time to time. It is imperative for a CA to define its business policies and practices in black and white and publish the same with approval of CCA. A CA audits is processes and infrastructure periodically regularly by established third party auditors for safety and security and to remain in business [15, 21].

A CA certificate holder can use certificate to sign or encrypt document while communicating it over INTERNET. A computer server can use CA certificate to establish Secured Socket Layer (SSL) connection for secured data packet exchange. Alternatively, Enterprise Certifying Authority can also be established with defined polices and practices for secured data exchange within a closed group/s with self signed certificates. Moving ahead, one may protect digital documents with water marks or can even embedded it in a cover (digital) object to hide the same from pubic glare. Hashing a document and storing the output safely allows one to verify it later for possible undesired spurious alteration. At enterprise level DNS, Firewall, Proxy Server configuration provides additional security. Individually, awareness and sensible usages of powerful digital tools provides defense that saves time, energy and money. As hackers and crackers sharpen their skill defenders too need to evolve new ways to defend digital wealth [15, 21].

VII. CONCLUSION

As technology advances, scope for Digital Security threat also increases, making digital security objectives a moving target. Constant vigil and exploration of path for defenses provides answer. Generally, IT security is based on prevention against known threats. Basic understanding of hacker's approach to attack helps us to prepare our defense models. However, it is difficult to plan a comprehensive and full proof defense mechanism where old tactics evolve and new tactics emerge in continuum. As technologies evolve the tactics for attack also advance. For attackers surprise remains the key strength. In recent years, motivation for attack is also changing from sheer financial gain or fun to serious business. Industrial, political and even personal gains too are motivating cyber mercenaries to organize attacks. This makes enactment of effective cyber law at national and international level along with continuous discovery of new defense technology. However, awareness and sensible use of technology too are essential to ensure growth and prosperity.

VIII. REFERENCES

[1]. Cortada J. W, Gupta A.M. Le Noir Marc; How Nations thrive in the Information Age, IBM Institute for Business Value, IBM Global Business Services,

[2]. Dutta Avijit; Knowledge Ubiquity in WEB 2.0 Paradigm; Innovation in Information System and Technology, ITCDC '09 Macmillan Publications; Page 234-238,

[3]. Dutta Avijit; Collaborative Knowledge with Cloud Computing, Proceedings of the 4th National Conference, INDIACom – 2010,

[4]. Dutta Avijit; Digital Communication and Knowledge Society; BIJIT – 2012 Issue 8: (July - December, 2012 Vol.4 No.2)

[5]. Dutta Avijit; Agile Social Interaction on Virtual Plane; Proceedings of the 7th National Conference; INDIACom-2013,

[6]. Jeffrey O. Kephart, David M. Chess, Autonomic Computing, IBM Thomas J. Watson Research Center, IEEE Computer Society 2003,

[7]. Kalle Lytinen, Youngjin Yoo, The Next Wave of Nomadic Computing: A Research Agenda for Information Systems Research, Working Papers on Information Systems, Sprouts, ISSN 1535-6078

[8]. Karlene C. Cousins, Daniel Robey; Human agency in awireless world: Patterns of technology use in nomadic computing environments; Information and Organization; Science Direct.

[9]. Krishna Venkatasubramanian and Sandeep K.S. Gupta, Security Solutions for Pervasive Healthcare P1: BINAYA DASH, December 8, 2006 11:58 AU7921 AU7921˙C015

[10]. L. Kleinrock ; Nomadic Computing; Computer Science Department Los Angeles, California, USA

[11]. Leonard Kleinrock NOMADIC COMPUTING - AN OPPORTUNITY CCR 4/95

[12]. Mark Burgin and Eugene Eberbach, Evolutionary Computation And the Processes of Life; an ACM publication August, 2012;

[13]. Ruth M Davis, Evolution of Computers and Computing, Science Vol. 195

[14]. Satyanarayanan M, .Pervasive Computing: Vision and Challenges; School of Computer Science Carnegie Mellon University

[15]. TechTarget, Security Media Group, Information Security, October 2014, Vol 16, No 8.

[16]. Tim O'Reilly and John Battelle; Web Squared:Web 2.0 Five Years On;Special Report

[17]. Thomas F. La Porta, Krishan K. Sabnani, Richard D. Gitlin; Challenges for Nomadic Computing: Mobility Management and Wireless Communications; Bell Laboratories

[18]. Weiser, M. The , The Computer for The 21st Century, Scientific American, September 1991, Pages 94-104

[19]. Weiser, M, Brown, J.S.The Coming Age of Calm Technology, TECHNOLOGY1 Xerox PARC October 5, 1996

[20].http://en.wikipedia.org/wiki/Transmission_Control_Protocol

[21].http://en.wikipedia.org/wiki/Public_key_infrastructure