Cyber Physical Systems (CPSs) – Opportunities and Challenges for Improving Cyber Security

Amit Kumar Tyagi
Research Scholar
Department of Computer Science and Engineering,
Pondicherry Engineering College,
Puducherry-605014, India

ABSTRACT

With increasing global reliance on the Internet as a medium, to make transactions and transmit information comes with an increased risk of cyber-attacks. Today’s Internet is using by various societies of all available sectors. It is implemented by rapid changes in computing technology and expanded internet prevalence. But in opposite of this, malicious activities are growing rapidly and the technique to protect internet is becoming very critical. Every country’s cyber infrastructure is interconnected with and instrumental to economic prosperity and national security. However, most of the cyberinfrastructures are not secure and are vulnerable to severe attacks. Several malicious actors potentially leading to failure of critical infrastructure, exploitation of sensitive information, and loss of intellectual property (for e.g. US White House 2009, US Senate 2010, and Iran 2010 etc.).

This paper introduces the idea of cyber physical system (CPS). Cyber-Physical Systems are integration of computation and physical processes. A cyber-physical system is a system of collaborating computational elements controlling physical entities. Today’s benefits of virtualization technology are that can obtain high resource utilization through dynamic sharing of physical resources. Today’s this virtualization technology has become a key technology for the next generation computing which can easily get information technology (IT) infrastructure anytime, anywhere and expand. This work introduces various essentials opportunities and future challenges to improve cyber security and building a CPS system more secure and powerful.

Keywords

Cyber Physical System, Cyber Security, Stuxnet, Threats.

1. INTRODUCTION

Modern life of human being is increasingly dependent on a multitude of interconnected and interdependent infrastructures. Today’s the inherent human desire for change, progress, mobility, entertainment, safety and security are leading the way to the development of intelligent automated systems (IAS). Driven by innovation, Intelligent Automation Systems believe technical know-how and application engineering make the difference. CPS or control systems are the most prominent enabling technology for IAS. A cyber physical system is an integration of physical world devices and cyber-world computing and communications capabilities, making the environment smarter. It enables cooperation, monitoring, coordination and control communication between the physical and cyber worlds [2]. In that, a cyber asset that denotes any hardware, software, or data that has value on an internet network. Cyber assets support missions with different priorities for every country. But cyber assets often have vulnerabilities that can be exploited by attacks and therefore, their security status may keep changing. Keeping the security level of assets at an acceptable level requires efficient continuous monitoring, risk assessment and resilience delivery in real time [5].

Moreover this, most defense, corporate, and civilian systems today are Internet-based. And the trustworthiness of Internet-based systems heavily depends on their security characteristics [6]. It has been forecasted by several national defense experts that the next big terrorist threat will be a cyber-war. Thus, strong data protection and efficient cyber risk management is the need of the hour today. Due to the effect of misaligned incentives between security product vendors, network users, and regulatory agencies, no security infrastructure work in a correct and secure manner [6]. Today’s Cybersecurity is inherently weak because it is missing the ability to defend the overall system instead of individual computers. Cybersecurity is a critical concern as society has become highly interconnected and reliant on a global system of computers, communication networks and software systems. Time to time different models and system for the protection of physical system have been proof by severe researchers. But till now, no model is perfect one.

The current strategies used in human and cyber security to protect (or handling threats) from malicious attacks are not capable in our increasingly interdependent world. Challenges in human security are changing through global terror networks [10]. Cybersecurity, by virtue of its rapid and hidden processes is arguably an even greater challenge that is poorly met by existing systems [11]. Today’s cybersecurity attacks are a major and increasing burden to economic and social systems globally.

The demands of addressing current challenges in human and cyber security are motivating for the development of fundamentally new approaches. An essential feature of new challenges is their distributed nature [11]. Global transportation and communication systems enable distributed groups of individuals to cause major physical or informational damage, elevating the global challenge of maintaining security at any location [3]. But traditional police forces with solely local authority cannot respond to global relationships and associations. Although cyberspace is the sum of various components i.e. include different sectors in it i.e. sometimes categorized as a discrete sector (such as food, water, health and transportation). In practice it is so deeply embedded into sectors such as energy and transport as to make any separation meaningless. Cyberspace can be visualized instead as a thin layer or nervous system running through all other sectors [12], enabling them to communicate and function. For e.g. the existence of this international asset database was revealed by WikiLeaks in 2010. As with the self-reporting (from state and local officials) in the National Asset Database, US embassies were asked to submit a list of critical infrastructure in their host country. The reliance on communication networks and standard communication protocols to transmit measurements and control packets increases the possibility of intentional and worst-case (cyber) attacks against physical plants [2, 9] and different sectors for e.g. the list of 259 sites included ordnance manufacturers, pharmaceutical corporations, and hydroelectric dams, suppliers of rabies vaccine, telecom providers and major ports. Fig. 1 shows the difference between cyber and normal information technology (IT) security.

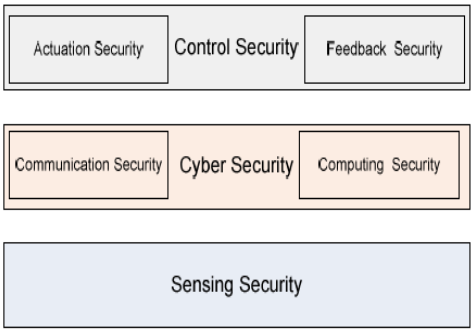

Fig. 1 relationship between cyber and control security

In current news, North Korea have did successfully test of Hydrogen Bomb and some other long ranges missiles. Which is a dangerous signal to the entire world. Many countries have implemented ban on North Korea. We know only some of the countries like India, America, China, Japan, Russia, South Korea etc. have only some cyber enabled technologies to fail their enemy’s movements. But this facility should be for every country, because in this world every county is an enemy for another one country. A country cannot trust on other countries. Today we need to protect cyber space, we need a secure infrastructure to run our business in a nation or among different countries. For that together we also need a system which is aware about current cyber security requirements and rules of this world. To understand the system rules, we need a system, who is more aware about these rules“? System Aware Cyber Security is defined as the utilization of reusable security techniques that are integrated into the system, creating a solution architecture that is designed with a specific application in mind and thus is able to provide unique security capabilities and address the threats of infections embedded in mission critical systems. This protection can be implemented through of variety of techniques i.e. capabilities to deter potential attackers, detect when the system has been compromised, isolates the subsystems that have been compromised, or restores the system to an original, uncompromised state.

Hence finally this paper organised as; Section 2 discusses about related work required for current cyber security system. Section 3 discusses about “why we should care about cyber security”? Section 4 discusses about “why current cyber security cannot work for the cyber physical systems”? Some future challenges in CPS are discussed in section 5. Section 6 discusses about future work related to control systems. Finally section 7 concludes this work in brief.

2. RELATED WORK

Cyber-Physical Systems arise from the tight integration of physical processes, computational resources, and communication capabilities i.e. processing units monitor and control physical processes [2] by means of sensor and actuator networks for e.g. transportation networks, power generation and distribution networks, water and gas distribution networks, advanced communication systems and control systems. Cyber-physical systems (CPS) have been at the core of critical infrastructures and industrial control systems for many decades, and yet, there have been few confirmed cases of computer-based (cyber) attacks [7]. Control systems are usually composed of a set of networked agents, consisting of sensors, actuators, control processing units such as programmable logic controllers (PLCs), and communication devices [13]. The objectives of such a control structure are: (1) to maintain safe operational goals by limiting the probability of undesirable behavior, (2) to meet the production demands by keeping certain process values within prescribed limits, (3) to maximize production profit. Control systems, are now at a higher risk to computer attacks because their vulnerabilities are increasingly becoming exposed and available to an ever-growing set of motivated and highly-skilled attackers.

So the need for cyber security has become apparent in the success of Internet fraud, including breaches of high security systems and theft of personal records. For a patient, leaking of his personal information can create a critical situation for him. The extent and variety of “cyber” actions has increased with the ubiquity of spam, spyware, phishing, zombie networks, denial of service attacks, etc. A spam-blocking service reports over 4.7 billion spam messages intercepted since November 2005 (also 10 million in 2011, and 25 million in 2015), i.e. almost ten times the amount of legitimate traffic over that particular period. For e.g. now a days every user on internet gets at least a single spam (at most 10) mail per day form a malicious attacker. Many of the spam messages advertise fraudulent products or otherwise attempt to defraud their readers; they contain links to unlawful sites, which also serves to skew search engines like Google in their favour; and they often originate from otherwise legitimate computers whose security has been compromised.

Today‘s Cyber-physical systems suffers from specific vulnerabilities which do not affect classical control systems, and for which appropriate detection and identification techniques need to be developed for e.g. Stuxnet worm, Aurora type of attack etc. The ultimate goal of Stuxnet is to sabotage that facility by reprogramming controllers to operate, most likely, out of their specified boundaries. Stuxnet demonstrates that the motivation and capability exists for creating computer attacks capable to achieve military goals [14]. The most significant of cyber-attacks on industrial control systems was Stuxnet, which happened in 2010. Stuxnet, a large complex piece of malware with many different components and functionalities, targeted Siemens industrial control systems and exploited four zero-day vulnerabilities running Windows operating systems [15]. As a result, 60 percent of Iranian nuclear infrastructure was targeted, hence triggering genuine fear over the commencement of cyber warfare (refer table 1, in Appendix A). Stuxnet not only cause devastating consequences [14], but also it is very difficult to detect (due to using Stuxnet zero-day vulnerabilities). No antivirus software would not have prevented from this attack. In fact, the level of sophistication of the attack prevented some well-known security companies such as Kaspersky to detect it initially. In addition, victims attempting to detect modifications to their embedded controllers would not see any rogue code as Stuxnet hides its modifications with sophisticated PLC rootkits, and validated its drivers with trusted certificates [2, 14]. Various people have criminal mind by birth and they used this gift in cyber-attack/illegal activities. Actually they have brilliant ideas to breaches a cyber system. Ideas are bulletproof and cannot be killed. They always work for the benefit for their nation/for themselves for financial gain. As discussed, Physical attacks in CPS used for extortion and terrorism. And cyber-attacks are a natural progression to physical attacks: they are cheaper, less risky for the attacker [13], are not constrained by distance, and are easier to replicate and coordinate.

Hence this section discusses about related work needed to improve the cyber physical system form physical attacks. Now next section will discuss about points regarding using cyber security in these physical systems.

3. WHY SHOULD WE CARE ABOUT CYBER SECURITY?

As discussed above, cyber security have an essential role to run CPS. Various information security methods, such as authentication, access control, message integrity, and cryptography methods, appear inadequate for satisfactory protection of cyber physical systems [2, 9]. From a policy perspective, there are at least five reasons "why users should care about cyber security"? First, there are a growing number of individuals who use the Internet, and many of these new users are unfamiliar with risks in cyberspace [16]. To illustrate, the number of Internet users around the world in 2000 was approximately 361 million; at the end of 2011, the figure had grown to 2.27 billion – more than a six-fold increase in a little over ten years. Second, the number of cyber-related applications has increased steadily over the past two decades i.e. a greater reliance on Internet-based services also attracts criminal groups which seek new avenues to make money. Criminal groups are continually exploring new ways to hack into technologies such as credit cards, automated teller machines (ATMs), and Radio Frequency Identification Devices (RFID). Third, critical infrastructures are becoming more vulnerable to cyber-attacks [16]. The Achilles heel of these infrastructures is their industrial control systems (ICS) such as supervisory control and data acquisition (SCADA) systems and distributed control systems (DCS). Connecting industrial control systems to the Internet has important implications. It exposes the control systems to hacking, worms, viruses, and a number of other vulnerabilities that can be introduced through the Internet, intranets remote dial-up, and wireless applications. For e.g. in 2010, the targeting of Iran's nuclear facilities via the Stuxnet [2, 16] virus demonstrated how a specific ICS could be sabotaged remotely. Fourth, malicious cyber activities are becoming more sophisticated and easier to execute. Individuals interested in mounting a cyber-attack do not need to have any advanced knowledge of computer programming, as they can purchase off the shelf crime kit tool ware. An example of such programmes is the Zeus crime kit whose malicious code can be customized. Fifth, there is a wide range of individuals and groups who may be interested in using cyber space for questionable objectives. While there is a tendency to focus on specific groups such as organized crime seeking financial gain and terrorists who might utilize the web to communicate and spread their ideologies [2, 17], there are other profiles of individuals who could threaten cyber security. These include organizations and groups interested in accessing sensitive information from government sources or international organizations.

3.1 Cyber Security Requirements

In general, the cyber security requirements of a system deployed in response to cyber threats includes three main properties: confidentiality, integrity and availability. Confidentiality prevents an unauthorized user from obtaining secret or private information. Integrity prevents an unauthorized user/attacker from modifying the information. Availability ensures that a resource is available to the legitimate user when needed. All properties can combined as in form of relationship (refer fig. 2):

Now Several Privacy Principles needed for improving Cyber Physical System for a better world. Generally Wang and Kobsa identify a set of 11 fundamental privacy principles [18] which can describe as:

1. Notice/awareness: Make policy statements clear and explicit.
2. Data minimization: Carefully evaluate the necessity, effectiveness and proportionality of a new technology before deployment. Prefer the least privacy-invasive solutions [18].

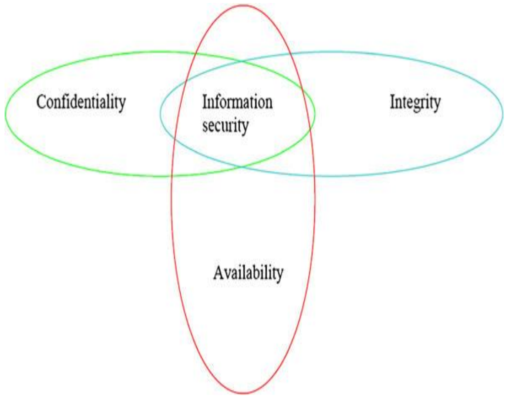

Fig. 2 Interaction of fundamental security requirements in a system

3. Purpose specification: Specify the purpose of data collection at the collection time.
4. Collection limitation: Set limits to the collection of data.
5. Use limitation: Personal data should not be used or disclosed for purposes other than those specified.
6. Onward transfer: Do not transfer data to a 3D party if it does not ensure adequate protection.
7. Choice/consent: Individuals should be provided with mechanisms, such as opt-in and opt-out mechanisms, to decide on the collection, use and disclosure of their personal data.
8. Access/participation: Individuals can access and inspect their stored data.
9. Integrity/accuracy: A data controller should ensure that the collected personal data are sufficiently accurate and up-to-date to the intended purpose.
10. Security: Protect data against risks such as loss, unauthorized access, destruction, use, modification or disclosure.
11. Enforcement: Include mechanisms to enforce privacy principles.

We believe that by understanding the interactions of the control system with the physical world, we should be able to 1) Better understand the consequences of an attack 2) Design novel attack-detection algorithms 3) Design new attack-resilient algorithms and architectures.

3.2 Current Cyber Security

There are a number of cyber security systems used by different – different countries to protect their resources from their enemies. But these systems are parallel in some way to perform several communications. Cyber security is totally differs from a traditional IT security [7]. In addition, there are specific efforts to adapt concepts from the physical system for cyber security. Now a days, cyber security needs three layers to protect human beings/internet users against cyber-attacks.

3.2.1 Layered defense

The first layer consisting of barriers in cyber security includes firewalls and the separation of distinct networks for e.g. ATMs and bank transactions [11]. In cyber security these include password authentication and S/Key challenges. These security systems prevent malware from entering a system as skin protects an organism. The second layer of cyber security includes detection of exploits and generic responses to them. This includes Domain Name Server Black Lists (DNSBL) often called Real time Black hole Lists (RBLs). These are services that gather and provide lists of internet protocol (IPs) that are sources of spam and other malware. Institutional mail servers can automatically implement policies that use this information to block domains on the Internet that are sources of spam [2, 11]. The sources of spam may include servers set up for this purpose, or zombies, botnet [1] (refer table 2, in Appendix A) etc. which are computers that have been compromised by malware so that they transmit spam and malware on behalf of others. In effect, zombies are the analog of virus infected cells that become factories for viruses and other pathogens. The large number of these exploits today results in a response which is akin to a generic immunity response. The third layer of cyber security includes virus scanners and e-mail filters are the analogs of the adaptive immune system. These applications search programs stored on disk or incoming e-mail messages for signatures of malware and spam. If the detection system is not specific enough, programs that are valid, and e-mail that is valid are rejected [11]. Alternatively, malware or spam may not be rejected. The desired versus undesired categories are analogous to the discrimination of "self" from "other" in the adaptive immune system. Where self consists of legitimate software and desired e-mail, and other is the malware (e.g. Virus, Trojan horse, etc.) which would compromise the system using spam. The existence of false-positives and false-negatives that misidentify whether the spam or malware are legitimate is similar to errors of classification in the immune system as well [2, 11].

3.2.2 Malware Detection

Prevention of a process is always cheapest in comparison of detection and fixing it. Detecting a malware is later thing, first learn to prevent from it (refer; some preventive and management measures in table 3, in Appendix A). Using awareness about using safe internet, we can prevent ourselves from severe malware attacks. A computer physical system must detect both known and unknown viruses and spam. For this purpose a program fragment or small piece of data from a larger set can be used as a detection template. This extracted data can be compared with correspondingly extracted data from a virus/spam. The latter is known as the "signature" of the virus/spam. Finding the "signature" within a piece of software indicates that the software has been infected. Various signatures can be constructed based upon procedures specified by individuals (heuristic rules), or statistical pattern detection (Bayesian filtering), and collaborative identification (when voluntary human communities manually specify spam signatures that are shared).

Some detection systems are local in that the software itself learns from labeling by the user "what is spam and what isn't"? In this case the user manually identifies spam, non-spam, and signatures that are extracted automatically. A user differentiate between the spam and non-spam by using software. Moreover this, to detect a deviant computer system that may be the source of other attacks, a pattern detection system has a representation of the types of patterns that can arise. Among these a set of "self-patterns" are created, representing the legitimate ways in which traffic can flow amongst the computers of a Local Area Network (LAN). Abnormal traffic, such as a computer suddenly sending thousands of e-mail messages to the external Internet, is a "non- self-pattern" and is considered a sign of infection [11] (in this example, the computer may have been co-opted by a spammer and used as a "zombie" to spread spam and malware). Further revisions arise after generated reports by a software due to the detection of the virus. Such detection occurs when individuals observe activity of processes on computers outside of normal operations, or of damage due to such processes.

Hence this section discusses about "how current security work for internet network and what is the use of cyber security now a days"? Now next section discusses about "why this type of cyber security/current cyber space are unwilling to protect cyber physical system"?

4. WHY CURRENT CYBER SECURITY CANNOT WORK?

Integration of physical processes and computing, of course, is not new. Today's cyber security systems need to provide some protection for malware and spam. Because the on-going presence of large volumes of spam and malware, and exploits, suggests that the existing protections are too limited in their abilities and requires greater attention to the principles of security as embedded in computer system operations which would give rise to improved outcomes [11]. Several physical attacks are measured on CPS which is generally used for extortion and terrorism i.e. hackers try to get the information of defense military of a country to gain financial gain (refer-Appendix A). This is also a co-incidence that in last five years, India's several top nuclear scientists have died unnatural death. This is not a coincidence, but here it is a matter of national security. Cyber-attacks are a natural progression to physical attacks because they are cheaper, less risky for an attacker, are not constrained by distance, and are easier to replicate and coordinate [13]. Still, we did not capture the dynamics of communication and interplay of detection and action that should provide better security and better self-protection against physical attacks. The limitations with current cyber security is to include the manner of detection and sharing of signatures of malware (local, centralized and limited distribution systems), as well as the limits in implementing actions to prevent or stop attacks and exploits. There are two fundamental reasons that the current approaches to cyber security cannot work effectively:

a) There is no mechanism for rapid pervasive distribution of security processes that can respond to new types of malware or spam [11]. One way to understand the ineffectiveness of security distribution is to compare the distribution of security with that of malware. Malware is much more pervasively and rapidly distributed than the security that is designed to guard against it. By contrast, there is no defensive analog of malware, in that the anti-malware software is centrally controlled instead of being distributed in origin. A better correspondence would be a security system that would operate on the basis of a peer-to-peer (P2P) protocol. A peer-to-peer system would open the door to more opportunities for malware [2, 11], but this architecture would give attackers and defenders equal capabilities, unlike the current situation where attackers have a wider range of options, with potentially much greater capabilities.

b) The current architecture of the Internet is based upon an internet protocol (IP) that transmits messages independent of their content with the help of routers. Each router reads the target destination specified by the message (packet) identifies a node to transfer the message to that will enable eventual delivery to the destination, and transfers it [11]. In this process, there is no evaluation of what the message contains. Individual messages may be lost in transmission due to network overload like distributed denial of service (DDoS) attack [3] (refer table 1, in Appendix A) etc., but not due to evaluation of the contents of the message. This implies that as far as the sender and receivers are concerned, the network is transparent.

Analogously, there is no protection in the medium of the Internet. The two fundamental limitations of the architecture of the Internet from a security perspective imply that there is no mechanism for a security system to prevent actions consisting of nodes attacking other nodes in the Internet. In considering the transfer of messages, it is important to recognize that a message is also an action that can be harmful. Collective security preventing attacks would require that the routers of the Internet themselves would need to have protocols that allow refusal of transmission based upon content or extrinsic information such as point of origin [11]. The routers of the Internet serve as the transmission medium for the nodes of the Internet. Further, if we consider each destination node of the network to be like a "home," and the network to be like the "streets", then from the point of view of security, this is equivalent to having no police on the streets or military at the borders. Each household, or individual, must defend him or herself, using means of protection (e.g. guns, sword, etc.) purchased from the market. That the protection is left to the individual home reflects the open nature of the Internet. Besides that, preventive action or removal is only possible if the originating node voluntarily participates in a security action. Without such participation, the best that can be done is to protect from attack at its destination. In order to develop an effective collective security system similar to the immune or human security systems, substantial architectural changes must be implemented. Such an approach was implemented against spam transmission early in the history of DNSRBLs. However, it appears to be abandoned due to some illegal use.

Generally a router based security system would curtail the "Right of transmission," which may be considered fundamental in discussions of "Freedom of speech" [11]. One option can be providing security over internet without using a router also. Absent a router based security system, is to enable automatic transmission of security software among all terminal (non-router) nodes of the internet [2, 11]. This would enable rapid and pervasive distribution throughout the system. This is a similar propagation to that of viruses and other malware. Such automated transmission might be considered to be less desirable than router based security, as it involves partial loss of control by owners of the activities on their computers in favour of security operations. Corresponding software capabilities exist in peer-to-peer systems, and in existing voluntary security communities. Thus far we have not discussed the use of human legal systems to pursue human originators of malware and spam. In this regard, there are difficulties inherent in international law for pursuing such attacks as crime. Different countries have different laws for cyber-crimes. Various awareness programs are also a major issues to protect human beings or internet users against cyber-crime. Criminal prosecution is a high cost and time effort that can be effective in disrupting non-normative activities but not in curtailing widespread actions. Indeed, the existing success in prosecuting Internet crime is limited.

To prevent cyber-attacks in this world, people should be self-independent on cyber/control systems because their dependency on these types of systems put a lot of risk. Hence this section discusses about "how current cyber security cannot work for internet network"? Now next section discusses about arises challenges in cyber physical system with respect to cyber security.

5. FUTURE CHALLENGES IN CYBER PHYSICAL SYSTEMS

Cyber-physical systems by nature is concurrent. Physical processes are intrinsically concurrent, and their coupling with computing requires, at a minimum, concurrent composition of the computing processes with the physical ones. In fact, Cleveland and Sun suggest several challenges for handling traffic data including: statistical tools and models for point processes, marked point processes, and time series that account for non-stationarity. While it is clear that the security of control systems has become an active area in recent years, we believe that, no one has been able to articulate what is new and fundamentally different in this field from a research point of view compared to traditional information technology (IT) security. Several challenges can be define in this section as:

5.1 Challenges in Physical Systems

No a days, inaccuracies in source documents is a major challenge. Often in online sources, entities are discussed with incorrect names. Particularly glaring examples are the erroneous, synonymous use of the terms "malware" and "exploit", and the use of "virus" as a blanket term for any malware. Currently, we should focus on accurately labelling the documents, which may not necessarily contain correct information for these reasons. Cyber security would require either or both as its major challenges:

(a) Making pervasive distribution of self-propagating but non-destructive security ware acceptable and create a developer community for such security ware.

(b) Modifying the protocols of internet routers to accommodate adaptive security software that would regulate internet traffic of other kinds and self-regulate. These modifications would alter the perspective of the "rights" of the Internet, the right of transmission and the right of any node to communicate to any other node of the system. Moreover this, an effective security system requires that this right be limited, as best as possible, to those who do not cause damage to the computer systems/physical systems.

5.2 Cyber Security Challenges

The widespread use of the Internet for communication and commerce (i.e. control systems, transportation networks etc.) has increased the need for cyber security. As discussed, control systems are autonomous decision making agents which need to make decisions in real time. While availability is a well-studied problem in information security, real-time availability provides a stricter operational environment than most traditional IT systems [7]. The property of control systems that is most commonly brought up as a distinction with IT security is that software patching and frequent updates, are not well suited for control systems. It shows that traditional IT is differs from cyber security. As importance of cyber security, todays computers introduced into medical operations might first be used for tracking appointments and keeping financial records. Then they might be used for sending prescriptions from physician to pharmacy. Additionally cyber system can be used for real time monitoring of procedures. Finally, they can be used for remote controlling of procedures also.

Cyber security challenges that target individuals or organizations may result in the loss of sensitive information, lead to financial loss, facilitate repeat attacks (including on critical infrastructures), or facilitate a distributed denial of service (DDoS) attack [1, 3]. In general, at least five cyber security challenges may affect individual users, which are define as:

a) Many users are unaware of "how their computers could be compromised by malicious software (malware)"?

b) Slow pace of national and international legislation to tackle malicious online activity and new forms of cybercrime. Lack of progress in this area enables attackers to exploit loopholes and develop new means to target users [16]. For example, limited harmonisation in international laws against cyber-crime and other online activities – such as sending spam – allow individuals or groups to transfer their activities to countries were national legislation against specific malicious activity is either weak or altogether missing.

c) Which is not too prominent today, is ensuring continuity of service/access to the Internet [16]? This challenge is likely to increase as societal dependence on cyber space grows. One dimension is the need to protect the physical backbone of the Internet. While the Internet was constructed to be robust, it has certain weaknesses. An example is the principal submarine cables that connect different countries and regions to the Internet. More than 90% of Internet traffic is carried via undersea fibre optic cables. There have been several cases of damaged or stolen cables which have impacted services to millions of users for time spans ranging from a few hours to several days. The disruptions to these undersea cables can take many different forms, for example:

   - In July 2005, a portion of the SEA-ME-WE 3 submarine cable, which is among the longest in the world, was disrupted so the majority of Pakistani voice and data communications were disrupted for several hours;
   - In 2007, pirates stole 11 kilometres of the T-V-H submarine cable, affecting millions of Internet users in Vietnam. Several optimal amplifiers were out of commission for approximately 80 days until replacements could be inserted;
   - In 2011, most of Armenia lost access to the Internet for roughly five hours when an elderly woman looking for copper in neighbouring Georgia accidentally damaged a fibre optic link while digging with a shovel [16].
   - Substantial portions of Georgia and Azerbaijan were likewise affected.
   - Beyond stolen or damaged hardware, countries themselves can affect Internet access. As was demonstrated during the Arab spring uprising in Egypt in 2011, officials were able to shut off Internet access to the population overnight. On 28 January 2011, Egypt went "offline" for approximately five days, demonstrating the ability to effectively shut off the access for a country. While such a move is a national prerogative imposed by government officials (refer table 3, in Appendix A), the impacts may be felt in neighbouring countries as business links and communications across borders are affected.

d) The self-similar structure of network traffic and the inherent dynamic nature of the Internet,

e) The rapid growth in the Internet, both in terms of the number of components and size of the traffic.

Further, there are several other critical challenges also which are unique to cyber security that requires a common-cause failures (CCF)-based foundation for scoring to be enriched before it can be effective. First, while CCFs can be addressed solely through diverse redundancy, as indicated earlier in the discussion of design patterns, security solutions must include additional solution components, that should go beyond the application of diversity, in order to fulfill its functions. Second, unlike CCF solutions, cyber security solutions attempt to deter, deflect, and restore a system against an intelligent adversary exploiting available vulnerabilities, including the capability to assess the cause of failure indeed being a cyber-attack. Finally, a variety of design patterns, including diverse Redundancy, can be integrated into solutions, thereby requiring a scoring methodology that establishes criteria for assessing and comparing the value contributed by the individual elements of the broader solution space.

Hence this section discusses about various challenges regarding cyber security and cyber physical system. As discussed todays internet is an essential part of human being. From a survey, every second person visiting internet daily in various forms via Facebook, WhatsApp, Google, etc. So today's cyber security also is an essential part of human being. Further next section discusses about future work have to be done in cyber physical system with respect to cyber security.

6. FUTURE WORK

As discussed above, we find out that the major research challenge for preventing the compromise of cyber physical systems is to identify ways in which asset owners and vendors of control systems will be motivated to follow best security practices [7]. A challenge in a system also a future aspects. So as future aspects, there are currently some efforts in this direction, in particular from the standards community. Further for a secure CPS, should be able to (a) Enabling pervasive distribution of self-propagating security-ware and creating a developer community for such security-ware, and (b) Modifying the protocols of internet routers to accommodate adaptive security software that would regulate internet traffic. During this work, we find out that there are several open research topics in area of cyber physical system which can be mentioned in point like:

a) *Networking issues*. Since CPS spans from wireless sensor networks (WSNs) to mobile to mobile (M2M) communications, a lot of interworking issues (for e.g. heterogeneous network architecture) have to be further designed.

b) *Design and verification tools*. The tools are necessary for supporting simulation and co-design, as well as achieving the automatic development process from modeling to code [19]. Unfortunately, the existing tools are not suited for CPS design.

c) *Security and privacy*. Since sensing data are no longer owned by local devices, security and privacy issues become more critical in CPS.

d) *Real-time capabilities*. For some of CPS applications (e.g. AEV with WSNs navigation), we must ensure that real-time performance meets the specific requirements. However, many factors, such as hardware platform, control methods and networking protocol, will affect response time.

e) *Cross-layer/domain optimization*. The CPS applications involve the information fusion of multiple domains and hierarchical architectures (for e.g. proposed EMF). The cross-domain/layer optimizations are quite crucial for ensuring system reliability and real-time response.

f) *Cross-domain interference avoidance*. Communication reliability is very critical when multiple devices coexist. For example, Wi-Fi, Bluetooth and Zigbee work on the same 2.4 GHz ISM band to possibly generate interference.

g) *Standards development*. CPS applications heavily depend on many advanced technologies across multiple industries. The required scope of standardization is significantly greater than that of any traditional standards development [2].

h) *QoS and cloud computing*. For future CPS, it is a challenge to minimize energy consumption and maximize QoS. Fortunately, the cloud computing techniques supported by ubiquitous connectivity and virtualization can greatly help in this aspect.

i) *Aviation security.* A complex socio-technical eco-system, it offers an opportunity to think beyond conventional methodologies to improve system performance in a way that, hitherto, would not have been possible. Now it is required to understand that ‘true’ foresight of latent vulnerabilities can only be achieved by a system which is ‘intelligent’ and ‘self-aware’, in other words to identify and modify hostile pathogens before they are exploited. The development of true foresight in aviation security systems is critical to the prevention of future terrorist attacks.

j) *Sybil attack [4]*. In this, attacker creates a large number of false entities and uses those entities to perform illegitimate activities i.e. they can refuse to cooperate in information dissemination. Sybil nodes can hijack requests from normal nodes and send back bogus information. Generally Defense against Sybil attacks/botnet in cyber physical system is known to be difficult. The current version of iDispatcher still does not have a systematic approach to it yet, and so issue also remains as our future work. iDispatcher is a planet-scale, flexible and secure information dissemination platform.

k) *Pollution and poisoning attack.* In a Distributed Hash Table-based P2P file-sharing system, nodes publish titles of files they intend to share. However, attackers can also publish the titles of files that either they do not have (index poisoning attack) or they have a corrupted copy of the file (pollution attack). When a benign node tries to download a file that has been advertised falsely by the attacker, it will fail to download the file or download a corrupted copy.

l) *Phishing.* It is attempting to acquire information (and sometimes, indirectly, money) such as usernames, passwords, and credit card details by masquerading as a trustworthy entity in an electronic communication [1].

m) *Pharming*. This is a hacker’s attack intended to redirect a website’s traffic to another, bogus site. Pharming can be conducted either by changing the hosts file on a victim’s computer or by exploitation of a vulnerability in domain name system (DNS) server software.

n) *Security of the cyber layer*. It is of great societal importance, yet the dense interconnections between sectors – facilitated by cyberspace – make it harder to decide “what to protect”? As transportation intertwines with food distribution and telecommunications, and as these and many others sectors are supported fundamentally by the finance and energy sectors, it is more difficult to draw clear boundaries between critical areas.

o) The ability of any part of the Internet to send messages to any other part of the Internet without encountering security systems implies that weakest elements can be attacked, compromised, or controlled to enable progressively larger infestation of the system. Moreover, there is no mechanism for blocking their attacks at point of entry into the Internet rather than at point of attack at another node.

Hence above described issue required to be done for cyber physical systems as future work. This section discusses about future work related to cyber physical system. Now next section concludes this work in brief.

7. CONCLUSION

To fully realize the potential of CPS, the core abstractions of computing need to be rethought. Here we assume that in cyber space, a country is protected from internal attacks but not from external. We have presented the current status of the field of secure control systems together using cyber security. We find out that cyber security is necessary part for every countries and its people. We mitigated various issues why current cannot work to secure control systems. Further this work proposed some new research challenges and future points based on the physical models (existed) of the process being controlled. Our research challenges are mostly unsolved and we believe that future research in these areas can provide an additional level of security to cyber physical/control systems. Now we are in a new era where providing secure and powerful cyber infrastructure will help us to protect many of lives and will provide different experiences to human beings that no one has provided before. So everybody is warmly invited to do their research in this area.

8. ACKNOWLEDGEMENT

The author would like to thank the reviewers for their useful suggestions.

9. CONFLICT OF INTERESTS

The author declares that there is no conflict of interests regarding the publication of this paper.

10. REFERENCES

[1] Amit Kumar Tyagi, G.Aghila, “A Wide Scale Survey on Botnet”, International Journal of Computer Applications (0975-8887), Volume 34– No.9, November-2011.

[2] Lalit Sharma, Amit Kumar Tyagi et al., “An Efficient Cyber-Physical Systems for Mobile Environments”, ICADET, ISSN 2250-2459 (Online), Volume 4, Special Issue 1, pp.203-208, February 2014.

[3] Amit Kumar Tyagi, S.K.Tyagi et al., “A Survey on Security Provided for DoS attack”, ICADET, ISSN 2277

128X (Online), Volume 4, Special Issue 2, pp.117-124, February 2014.

[4] Amit Kumar Tyagi, Dr.N.Sreenath," Exposing and Classifying Various Attacks on Vehicular Ad-hoc Networks", ICADET, 21-22 February 2015.

[5] Hasan.C et al., Mission assurance policy and risk management in cybersecurity, 30 August 2013, Springer Science Business Media New York, 2013.

[6] http://www.scf.usc.edu/~rpal/RESSTR1AAA.pdf

[7] Alvaro A. C´ardenas, et al. Challenges for Securing Cyber Physical Systems, Workshop on Future Directions in Cyber-physical Systems Security, DHS, 23, July, 2009.

[8] Eric Ke Wang, et al., Security Issues and Challenges for Cyber Physical System, 2010 IEEE/ACM International Conference on Green Computing and Communications.

[9] Fabio Pasqualetti, Florian D¨orfler, and Francesco Bullo, Attack Detection and Identification in Cyber-Physical Systems – Part I: Models and Fundamental Limitations, IEEExplore, 2013.

[10] www.cybersecurityresearch.org/documents/CSRA_Workshop_Report.pdf

[11] http://arxiv.org/pdf/1303.2682.pdf

[12] www.chathamhouse.org/cyber2013

[13] https://www.usenix.org/legacy/event/hotsec08/tech/full_papers/cardenas/cardenas_html/

[14] Alvaro A. Cárdenas et al., Attacks against Process Control Systems: Risk, Assessment, Detection, and Response, ACM, 2011.

[15] Siddhartha Kumar Khaitan, James D. McCalley, Chen Ching Liu, Cyber Physical Systems Approach to Smart Electric Power Grid, (Book)

[16] https://www.ciaonet.org/attachments/21111/upl-oads

[17] Chopra Leena, Lamba Tripti, A Study of Cyber Security in Web Environment, IITM Journal of management and IT, 2014, Volume : 5, Issue 1.

[18] https://www.ics.uci.edu/~kobsa/.../2008-Handbook-LiabSec-kobsa.pdf

[19] http://www.doiserbia.nb.rs/img/doi/1820-0214/2013/1820-02141300018W.pdf

11. APPENDIX A

Table 1 Select Countries Targeted by Cyber Operations

Country	Attack Type	Date
Estonia	Distributed denial of service (DDoS	April-May2007
Lithuania	DDoS	June-July 2008
Georgia	DDoS	August 2008
South Korea	DDoS	July 2009
United States	Espionage	July 2009
Iran	Sabotage	July 2010
Internet Censuring e.g. China , Iran, Syria, Egypt	Restriction to internet access	Multiple Dates

Table 2 Actors who may threaten Cyber Security, Motivation, and Type of Attack

Group	Motivation	Type of Attack
Script kiddies	Curiosity / reputation	Readily available software
Hackers	Challenge of breaking new defenses financial gain	Use of automobile tools potential for coordinated attacks
Insiders	Revenge / extortion	Multiple possibilities
Hacktivists	Propaganda(social, political, economic, religious)	Same as script kidders/ hackers
Criminal groups	Financial gain	Phishing, pharming, spam
Spyware / malware authors	Many financial gain	Same as criminal groups
Botnet operators	Financial gain/cause disruption	Use of remotely controlled systems
Terrorists	Propaganda (political, social, economic, religious, cause disruption/damage)	Multiple possibilities including attacks on critical infrastructure
States	Cause disruption / damage espionage/ gather intelligence	Multiple possibilities

Table 3 Examples of Preventive and Consequence Management Measures

	Preventive Measures	**Consequence Management**
Technical Measures	Awareness raising, installation of protective software, use of black and white lists, use of open source software, introduction of new protocols (for e.g. IPv6), use of encryption	Increase bandwidth, filter incoming internet traffic, block access to incoming internet traffic, shift server usage, setting up ”redundant” systems
Institutional Measures	Establish CERTs and CSIRTs, create specialized agencies/bodies (for e.g. ENISA),organize table top exercises(e.g. cyber storm), introduce legislation and conventions, promote public private partnerships, consider need for a national cyber security strategy	Set up cyber “fire-brigades’, promote national synergy vis-à-vis cyber security, engage in international cooperation, apply legislation