IIT KHARAGPUR

NPTEL ONLINE CERTIFICATION COURSES

Industry 4.0: Cybersecurity

Dr. Sudip Misra

Professor

Department of Computer Science and Engineering

Indian Institute of Technology Kharagpur

Email: smisra@sit.iitkgp.ernet.in

Website: http://cse.iitkgp.ac.in/~smisra/

Research Lab: cse.iitkgp.ac.in/~smisra/swan/

What is Cybersecurity?

- In computing, security consists of
  - Cybersecurity
  - Physical security

- Protection of internet-connected systems from cyber-attacks is known as cybersecurity.

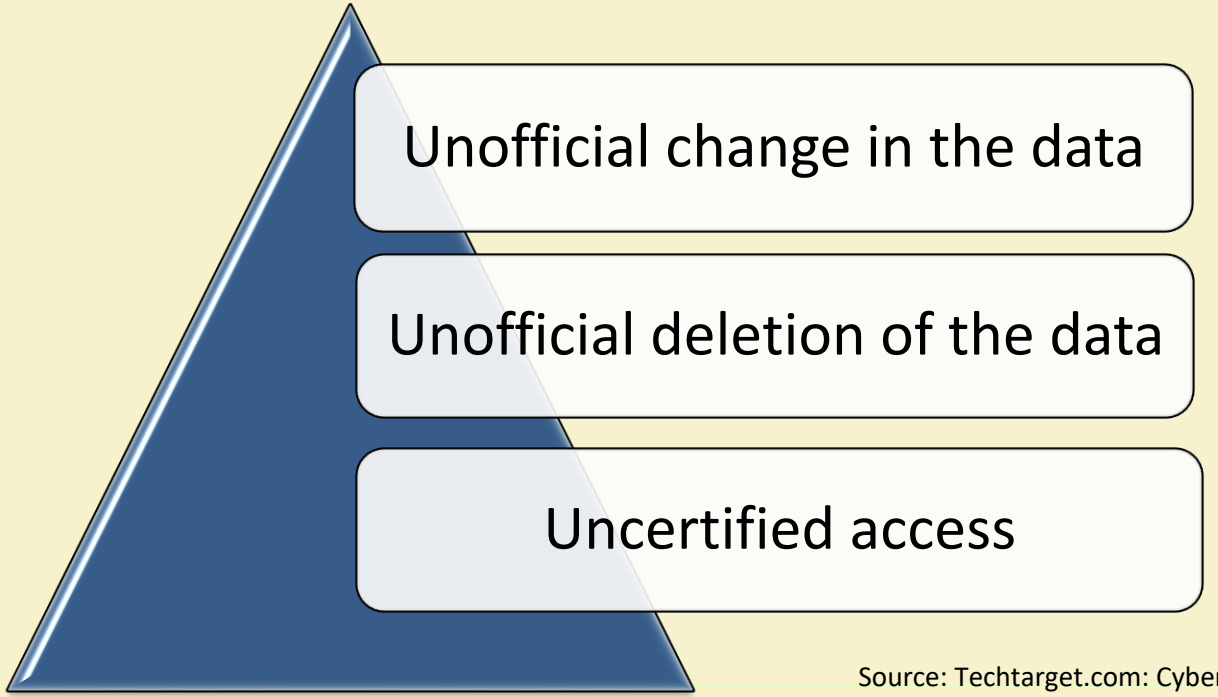
Source: Techtarget.com: Cybersecurity

What is Cybersecurity?

- This protection involves protection of
  - hardware
  - software
  - data
- Enterprises use cybersecurity and physical security simultaneously against unofficial access to data centres.

Source: Techtarget.com: Cybersecurity

Protect against what?



Source: Techtarget.com: Cybersecurity

Components of Cybersecurity

- Application Security
- Information Security
- Network Security
- Operational Security
- End-user Education

Source: Techtarget.com: Cybersecurity

Elements of cybersecurity(Contd.)

- Application security
  - It ensures the protection of applications from outer threats.
  - Some software, hardware and procedural methods are used for protection.
  - Some actions are needed to certify application security; these actions are known as countermeasures. There are two types of countermeasures.
    - Software countermeasure: application firewall
    - Hardware countermeasure: router/proxy

Source: Techtarget.com: Cybersecurity

Elements of cybersecurity(Contd.)

- Information Security
  - Information security is recognized as a subset of cybersecurity.
  - A set of strategies is known as information security, which handles some tools and policies. These policies filter the threats.
  - These strategies help maintain the availability, integrity and confidentiality of business data.

Source: Techtarget.com: Cybersecurity

Elements of cybersecurity(Contd.)

- Network Security
  - Network security is a process by which we take physical and software actions for protecting the network architecture.
  - It provides protection from unofficial access, improper use, fault, deletion, demolition.
  - Create a protective platform for users and computers.
  - It combines multiple layers of defences at the edge and in the network.

Source: Cisco: Security

Elements of cybersecurity(Contd.)

- Operational Security
  - Operational security (OPSEC) is an analytical action which categorizes information benefits.
  - For protection of these information benefits, it regulates the control.
  - Protection is an important factor in business perspectives; because of this OPSEC operations are commonly used in business actions.

Source: Cisco: Security

Elements of cybersecurity(Contd.)

- End-User education
  - End-users are the biggest security risk for an industry. They are the first to compromise the security.
  - Employees do not have all information about all the attacker, hence they can easily open the doors for the attackers.
  - As cybercrimes are increasing, it will be more important for industry to educate their employees about cyber-attacks.

Source: Cisco: Security

Types of Cybersecurity threats

- Ransom-ware
  - It provides a facility to the attacker in which the attacker locks the user's computer files by using an encryption and demand some money to unlock them.
  - Example: Locky
- Malware
  - A computer program which is used to disturb the computer user, such as computer viruses, spyware etc.
  - Example: Trojan Horse

Source: Techtarget.com: Cybersecurity

Types of Cybersecurity threats(Contd.)

- Social Engineering
  - This attack involves human interaction to mislead users.
  - It breaks security policy to get critical information, which is typically secured.
  - Example : Watering hole and Pretexting.
- Phishing
  - Phishing is in the form of false information. These information are basically false emails which have been sent through recognizable sources.
  - The aim is to get critical data, such as login information or credit card information.
  - Example: Google docs Phishing and Dropbox Phishing.

Source: Techtarget.com: Cybersecurity

Industrial Internet (II)

- Internet of things, computers and people, machines all together make Industrial Internet.
- It enables industrial intelligent actions to use advanced data analytic tools for gettable business results.
- Autonomous cars, intelligent rail-road systems are applications of industrial internet.

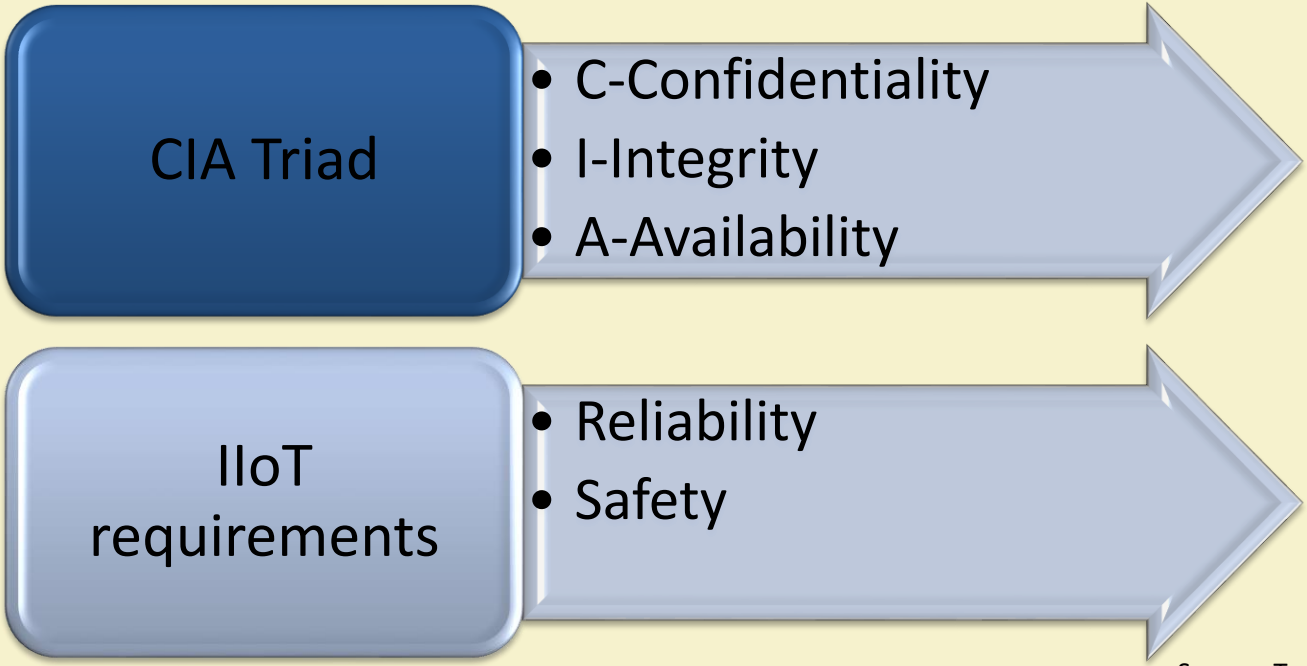
Source: i-scoop.eu : Cybersecurity-IIoT

Why IIoT Security Standards is required?

- Industries will need to use diverse systems and equipment but everything will be integrated on smart factory floor.
- Legacy systems must be brought under implementation.
- Every weak line in the chain puts whole factory at risk.
- Leaving security at the hands of individual IIoT implementers is dangerous.

Source: i-scoop.eu : Cybersecurity-IIoT

Cybersecurity Requirements



Source: Techtarget.com: Cybersecurity

CIA Triad

- C-Confidentiality
  - Confidentiality stops unauthorized disclosure of Information.
- I-Integrity
  - Integrity ensures that data cannot be changed in any unauthroized manner.
- A-Availability
  - Availability guarantees that information must be available only to the authorized user.

Source: Techtarget.com: Cybersecurity

Cybersecurity: Challenge in IIoT

- Cybersecurity has a major role in digital economy and it certainly is a big challenge in IIoT as well.
- In current digital transformation, capabilities such as manufacturing, logistics, shipping, healthcare and industries, which comes under the industrial internet, data breaches can occur, which increases different kinds of cybercrimes and cyber threats.

Source: Cybersecurity for industry 4.0: Thames

Cybersecurity for Industry 4.0

- Traditional cybersecurity mechanisms have the characteristics- confidentiality, authenticity, integrity, non-repudiation and access-control.
- These methods provide safety in network and computer attacks.
- The **new internet security** deals with **other attacks** which are capacious and very fast.
- Some methods are required for Industry 4.0 systems which enables automatic detection to cyber-attacks.

Source: Cybersecurity for industry 4.0: Thames

Cyberattack Detection: Methodologies and Algorithms

- Computational Intelligence systems (CIS)
  - An algorithm is required for CIS which combines and filters the data. This data is created by different types of events in a cyber domain.
  - Cyber-attack recognition systems deal with extensive volume of big dimensional data along with uniform advancing attack features.
  - CIS have become reasonable preferences to build new categorization algorithms for detection systems.

Source: Cybersecurity for industry 4.0: Thames

Software-Defined Cloud Manufacturing Architecture (SDCMA)

- There are mainly three parts of SDCMA
  - Software Plane
  - Hardware Plane
  - Ensemble Intelligence Framework (EIF).
- Software plane consists of control elements (CE).
- CE are used as data tap points, since they have deep observation into the communications and activities.

Source: Cybersecurity for industry 4.0: Thames

SDCMA(Contd.)

- In SDCMA, the streaming data is supplied to EIF by CE.
- Sensed data is detected by EIF.
- EIF is also responsible for detecting abnormality.

Source: Cybersecurity for industry 4.0: Thames

References

[1] Thames L. & Schaefer D.(2017). Cybersecurity for Industry 4.0: Analysis for Design and Manufacturing.Springer.

[2] Li BH, Zhang L, Wang SL, Tao F, Cao JW, Jiang XD et al. (2010) Cloud manufacturing: a new service oriented networked manufacturing model. Comput Integr Manuf Syst 16(1):1–7

[3] Ghorbani AA, Lu W, Tavallaee M.(2010) .Detection approaches. Springer, J Network Intrusion Detection and Prevention.

[4] https://searchsecurity.techtarget.com/definition/cybersecurity.

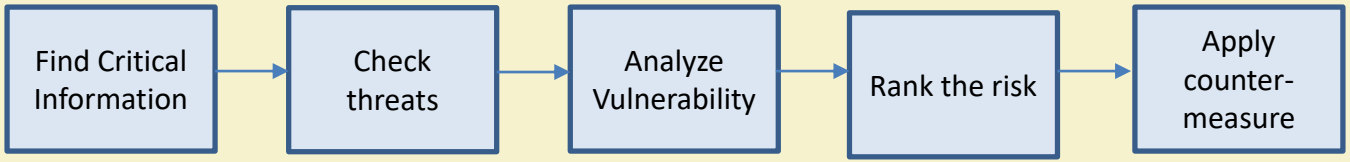
[5] https://www.cisco.com/c/en/us/products/security/what-is-network-security.html

[6] https://www.i-scoop.eu/internet-of-things-guide/industrial-internet-things-iiot-saving-costs-innovation/cybersecurity-industrial-internet-things/

[7] Xu X.(2012).From cloud computing to cloud manufacturing. Rob Comput Integr Manuf 28(1):75–86.

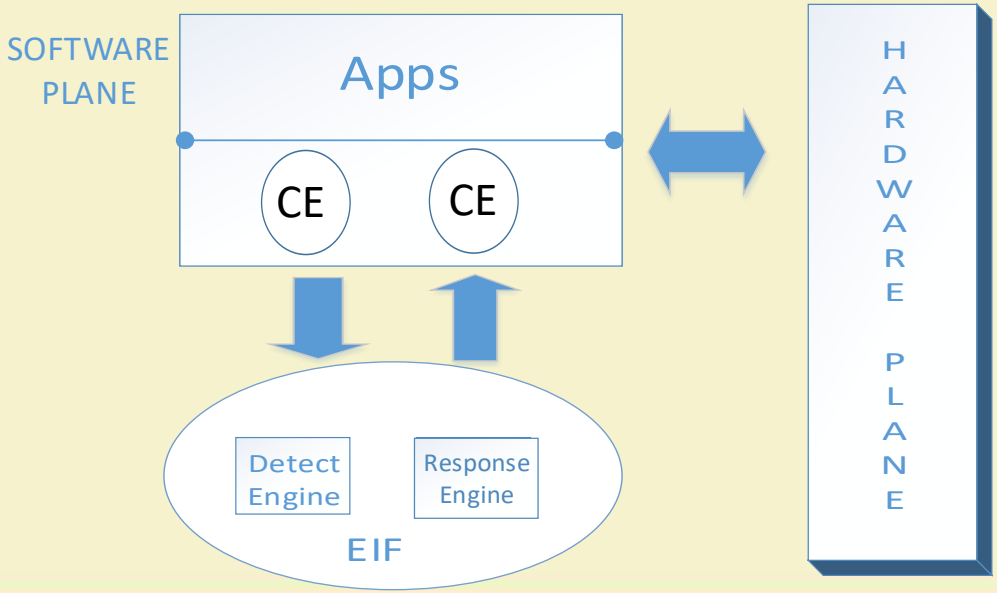
Thank You!!

9th Slide (Operational Security)



20th Slide

- SDCMA(Software Defined Cloud Manufacturing Architecture)



Ref.: Thames L., and Schaefer D.(2017).Cybersecurity for Industry 4.0: Analysis for Design and Manufacturing. Springer