

Regulation and Policy in the Telecommunications Industry TM 612-WS

By Dr. Raziq Yaqub
dr.raziq@gmail.com

Dr. Raziq Yaqub

Lecture—14

Warning
This Material MUST NOT BE
Copied, Reproduced or Forwarded

Dr. Raziq Yaqub

Contents

1. What is the Landscape of Cybersecurity?
2. How SECURITY Evolved to CYBERSECURITY?
3. Why Cybersecurity is a Challenge?
4. Some Worth Mentioning Attack Types
5. How to defend the attacks
6. Regulations on Cybersecurity

3

1 What is the Landscape of Cybersecurity?



What is the Cost of Developing a Stealth Bomber?

~ \$2B



Cost of Developing a Cyber Weapon?

~ Free



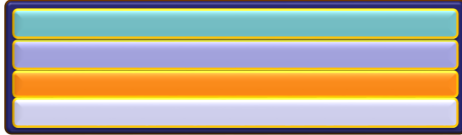
How Many Countries?

Are Engaged In a Cyber Arms Race?



~ 160+

Who Sponsors the Attacks?



Who Sponsors the Attacks?

Terrorists:	To Sabotage
Groups:	For financial benefits
Companies:	To stay ahead of competitors
Governments:	To spy for its own security/safety

Who is Vulnerable?



Airline Industry



Financial Industry



Telecom Industry

Almost everyone is vulnerable



Health Industry



Power Industry



Governments

What is the Cost of Damage from a Cyberattack?

Financial Damage

Down-time Cost (Per Hour):

- ATM Fees \$14,000
- Package shipping \$28,000
- Tele-ticket sales \$69,000
- Airline sales \$89,500
- Catalog sales \$90,000
- Credit card authorization \$2.6 million
- Brokerage operations \$6.24 million

Source: Contingency Planning Research

Is this the limit?
NO,

Loss of Reputation

Loss of Customer's trust

Example?



What are the Questions when attack happens?

Whenever Attack happens,
It Raises Several Important Questions

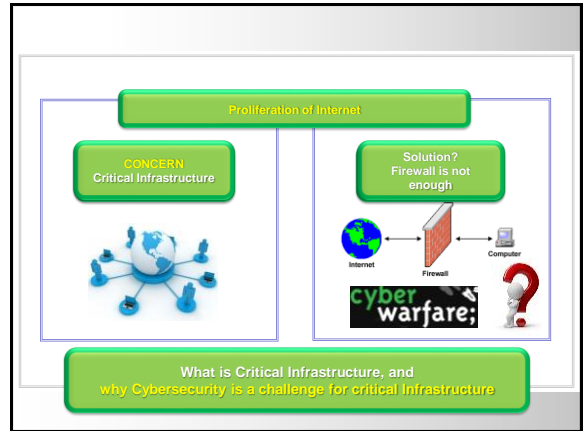
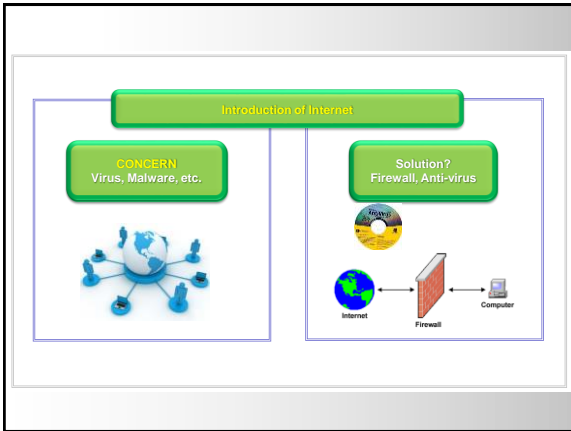
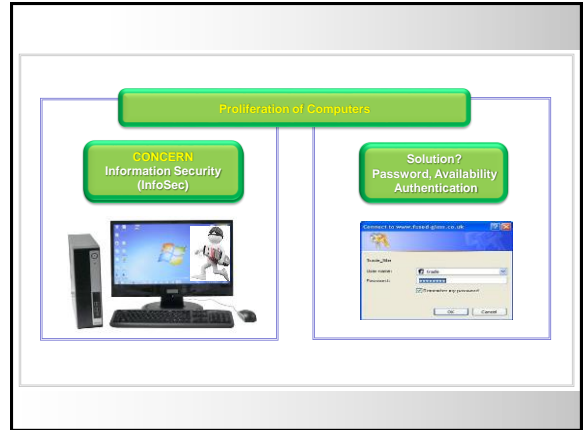
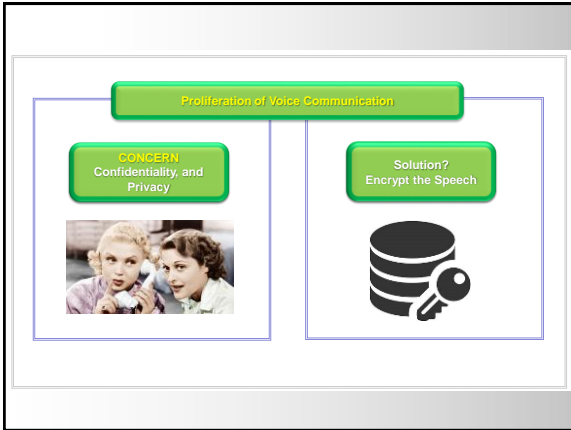
1. What information was taken, and who took it?
2. When and how did the attack occur?
3. Is it an internal or external attack?
4. What's the impact of this attack on the business?
5. How do we prevent recurrence?



Too Many QUESTIONS !!!!

2 How Security Evolved to Cybersecurity?











3

Why Cybersecurity is a Challenge for Critical Infrastructure



Cybersecurity is a challenge for critical Infrastructure

 <p>Boden Incident Power System Hacked Using Wi-Fi</p>	
 <p>Siberia Incident 3,000 Ton Explosion using Malware</p>	
 <p>Queensland Incident Millions of liters of untreated sewage released using Wi-Fi</p>	

Cybersecurity is a challenge for other actors as well

Hacking \$\$\$



Car Hacking



Intrusion in Health



Plane Drifting



Cyber security Threats are
Continuously Evolving

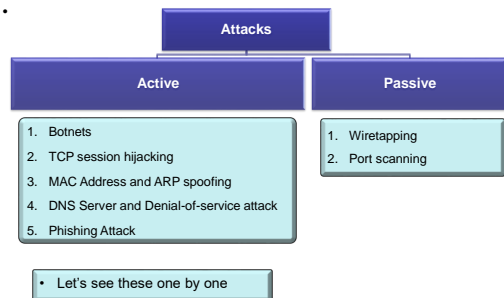


And so must our DEFENSE too



4 Some Worth Mentioning Attack Types

Types of Network Attacks



4 Some Worth Mentioning Attack Types

Botnet Attack

1. Botnet

- **Botnet**
 - A botnet consists of **bots**
 - Bots are programs installed on the machines of unaware Internet users
 - These bots receive commands from a **bot controller**



- **Attack Scenario**

- Botnet attacks do not target communications links
- But users machines/information

4

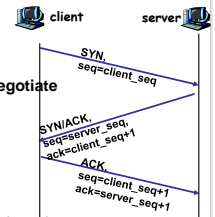
Some Worth Mentioning Attack Types

TCP Session Hijacking

2. TCP Session Hijacking

• In TCP connection, each packet has:

- Sequence (Seq) number and
- Acknowledgement (Ack) number



• Upon TCP connection setup, both ends negotiate

- The Seq number and
- The Ack number

• seq and ack number size is small (2^{32})

- Small size makes it easier to Guess the seq/ack numbers
- Thus easy to Hijack an already setup TCP connection

2. TCP Session Hijacking (Contd.)

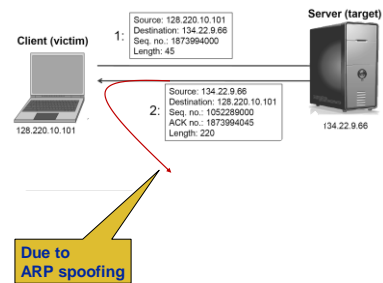
• Hijacking is Possible when

- An attacker is on the same network as the target machine
- Attacker can sniff all back/forth TCP packets and know the seq/ack numbers
- Attacker tries to inject a packet with a guessed seq/ack numbers with the spoofed IP address
- If he is successful in doing so, he can launch an attack



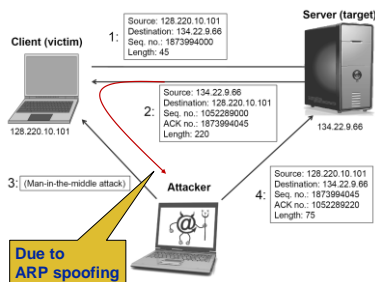
28

2. TCP Session Hijacking (Contd.)



29

2. TCP Session Hijacking (Contd.)



30

4

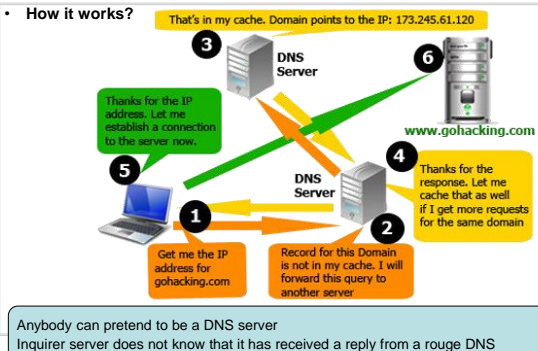
Some Worth Mentioning Attack Types

DoS & DDoS Attack

4. Domain Name System (DNS)

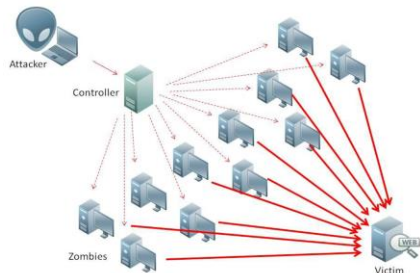
- DNS
 - It maps host names to IP addresses (and vice versa)
 - (i.e. looks up IP address for host name, and host name for IP address)
 - It performs basic authentication, as it was designed for a friendly environment

4. Domain Name System (DNS) (Contd.)



4. Domain Name System (DNS) (Contd.)

- DoS/DDoS (Distributed DoS) Attacks



4 Some Worth Mentioning Attack Types

Phishing Attack

Darkside's Attack

DarkSide Targeted Gas Pipeline with Phishing Attack

- DarkSide sent Phishing emails with malicious attachment
 - Someone clicked on the attachment that installed a malware on his computer
 - DarkSide took control of the email recipient's PC
-

Darkside's Attack

Once they took control of the email-recipient's PC,

- DarkSide performed ARP Scan to discover servers in the organization

ARP = Address Resolution Protocol,
It is used to discover Layer 2 addresses



- Through ARP Scan DarkSide discovered Domain Controller's address
 - Domain Controller is a critical server. It authorizes users access to network resources

Darkside's Attack

Once they discovered Domain Controller's address


- DarkSide tried to get escalated privileges
- DarkSide was successful in obtaining domain administrative credentials



Darkside's Attack

Once they obtained domain administrative credentials, then


- DarkSide sent SQL EXEC commands
 - SQL is a specialized query language for updating, deleting, and requesting information from databases
- DarkSide, by using SQL,
 - Attacked the billing system and disc



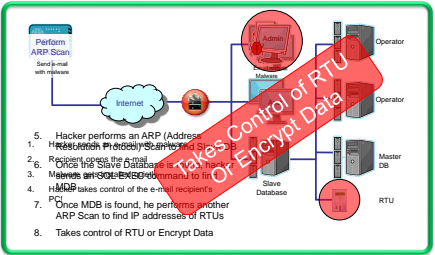
Darkside's Attack

Once they obtained domain administrative credentials, then

- DarkSide also Deployed ransomware attack that used Salsa20 and RSA-1024 encryption
 - It Exfiltrated Sensitive data
 - It encrypted victim's files
- DarkSide also Threatened
 - "If the ransom not paid, they will public the information"
 - Disable the RTUs (Remote Terminal Units)




5. Phishing Attack



- Hacker performs an ARP (Address Resolution Protocol) Scan
- Recipient opens the e-mail
- Once the Slave Database is found
- Hacker performs an ARP scan to find IP addresses of RTUs
- Hacker takes control of the e-mail recipient's PC
- Once MDB is found, he performs another ARP Scan to find IP addresses of RTUs
- Takes control of RTU or Encrypt Data

5 How to Defend the Attacks



Dr. Raziq Yaqub

Implement 5 Pillars of Security in the Security Architecture



Encryption



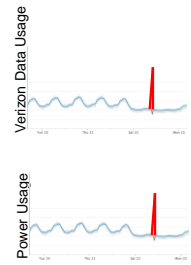
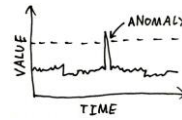
MEET ME IN THE PARK

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

NFFU NF JO UIF QBSL

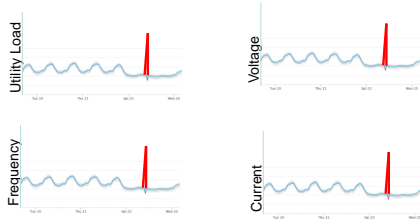
Anomaly Detection

- **Anomaly**
 - Something that deviates from what is standard, normal, or expected



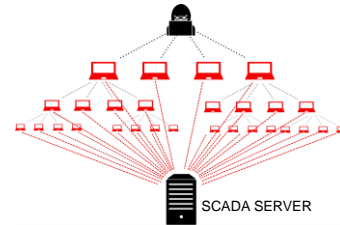
Anomaly is a Popular way of threat detection

- Following anomalies can be used for threat detection
 - Power System Parameters Anomaly
 - (such as Load, Voltage, Current, frequency, etc.)



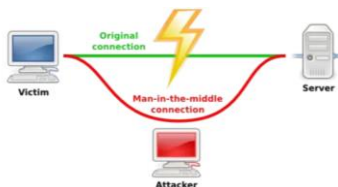
Anomaly is a Popular way of threat detection

- Following anomalies can be used for threat detection
 - Protocol Anomaly:
 - Power system specific protocols, (such as, SCADA DNP3, Modbus)



Anomaly is a Popular way of threat detection

- Following anomalies can be used for threat detection
 - Protocol Anomaly:
 - Communication system specific protocols (such as, IP Spoofing, MAC Spoofing)

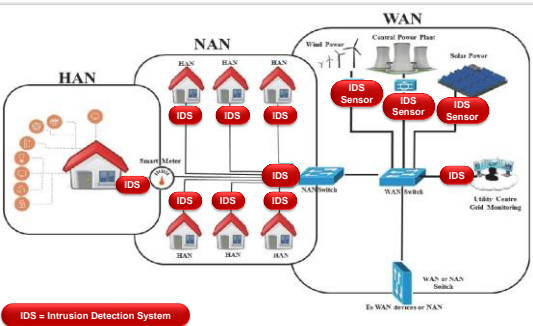


Signature Based Intrusion Detection

- Detection of attacks by looking at:
 - Specific patterns
 - Byte sequences in network traffic
 - Known malicious instruction sequences used by malware



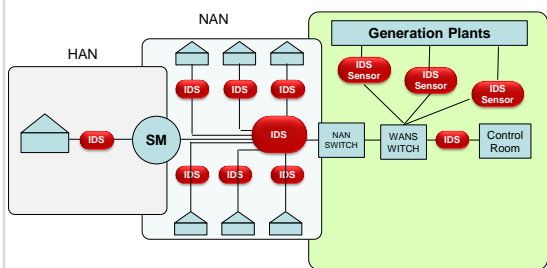
Intrusion Detection Framework Architecture (example Power System)



Dr. Raziq Yaqub

Intrusion Detection Framework Architecture (example Power System)

Block Diagram



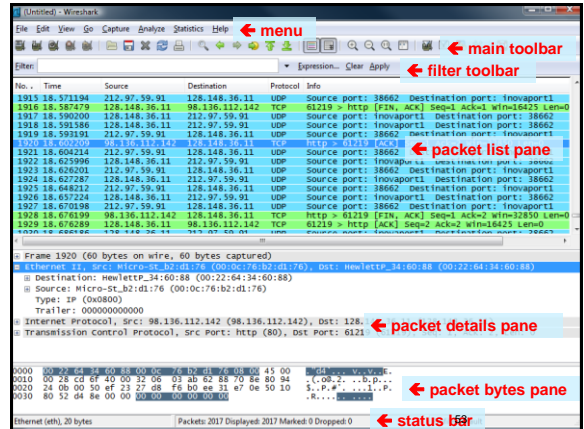
Dr. Raziq Yaqub

Wireshark

- Wireshark is a free and open-source packet analyzer.
- Wireshark uses pcap to capture packets
- It runs on Linux, macOS, and Microsoft Windows

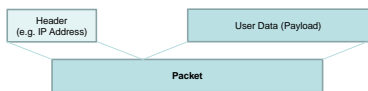


Dr. Raziq Yaqub



Deep Packet Inspection (DPI)

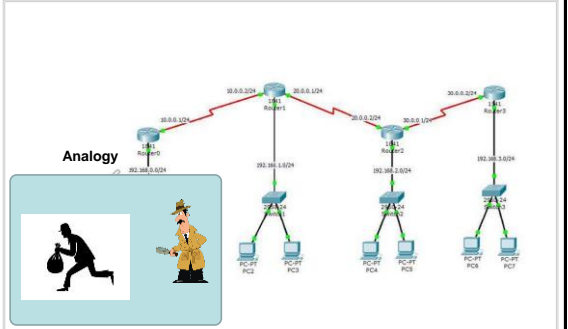
- Examining data packets (Packet as well as Header) as they pass an inspection point:



- Searching for
 - Protocol
 - Non-compliance
 - Viruses
 - Spam
 - Intrusions



Packet Tracing



Avoid Zero Day

- **Zero-day**
 - Is a computer-software vulnerability
 - Does not have any mitigation, remedy, or patches, because the developer/victim has just learned about the flaw
 - "Day Zero" is the day on which the victim learns of the vulnerability
- **Zero-day Attack**
 - An exploit directed at a zero-day is called a zero-day attack
 - Zero-day attacks are a severe threat



Dr. Raziq Yaqub



5 Cybersecurity is our Shared Responsibility

Cybersecurity is a shared responsibility

Each of us has a role to play

Only a single infected computer can infect thousands and perhaps millions of others

If everyone takes basic measures it can improve both individual and our collective safety online



Some steps you can take are:

Don't open emails or attachments that look suspicious

Set strong passwords, don't share them with anyone

Install necessary updates

Don't share too much personal information online



5

Regulations on Cybersecurity

Dr. Raziq Yaqub

Importance to Understand Cybersecurity Laws

- **Cybersecurity Laws are introduced to:**
 - To improve organizational security
 - To protect people and their assets
 - To mitigate Cyber Crimes
- **Every country has its own set of laws**
 - Governments have laid down security compliance requirements

60

Importance to Understand Cybersecurity Laws

- **Organizations must**
 - Incorporate the cyber laws as part of their security policy
 - Comply with the laws depending on their business
 - Understanding cyber laws and regulations helps firms avoid lawsuits, loss of public trust and reputation, and unnecessary down time

61

Importance of Legal Framework

- Law takes the principle of territoriality as point of departure;
- Cyber security tools and targets are physical-boundary-independent;
- Agreements between nations create a general common basis for cyber security measures

Dr. Raziq Yaqub

USA Cybersecurity Laws

- **Computer Fraud and Abuse Act (CFAA)**
 - Whoever ... intentionally accesses a computer without authorization or exceeds authorized access and thereby obtains... information from any protected computer ... as provided in subsection (c) of this CFAA
- **Electronic Protected Health Information (ePHI)**
- **Health Insurance Portability and Accountability Act (HIPPA)**
 - It protects information about individuals identifiable health records
 - It protects information both in motion and stationary

Dr. Raziq Yaqub

USA Cybersecurity Laws

- **Cybersecurity Enhancement Act 2014**
 - Public-Private Collaboration on Cybersecurity
 - Cybersecurity Research and Development
 - Education and Workforce Development
 - Cybersecurity Awareness and Preparedness
 - Advancement of Cybersecurity Technical Standards
- **National Cybersecurity Protection Act 2014**
- **Cybersecurity Workforce Assessment Act 2014**
- **Payment Card Industry Data Security Standards (PCI DSS)**
- **The Economic Espionage Act of 1996**

Dr. Raziq Yaqub

Privacy Protection Laws/Acts

- **Laws on corporations: HIPAA, HITECH, GLBA, PIEDA**
- **Laws on government: FPA, VA ISA, USA PATRIOT**

Dr. Raziq Yaqub

- **Illegal access**
- **Illegal interception**
- **Data interference**
- **System interference**
- **Misuse of devices**
- **Computer-related forgery**
- **Computer-related fraud**
- **Offences related to child pornography**
- **Offences related to infringements of copyright and related rights**

Dr. Raziq Yaqub

Liability

- **Personal Information**
 - Legally recognized obligation
 - Failure to conform to the required standard
- **Proximate causation and resulting injury or damage**

Dr. Raziq Yaqub

Chapter Review Questions (CRQ)

Chapter-14



Q1

- **Select the best statement**
- **Cost of developing cyber weapons**
 - A. Is almost equal to the cost of developing traditional war weapons
 - B. Is almost negligible compared to the cost of developing traditional war weapons
 - C. Is much higher than the cost of a stealth Bomber
 - D. Is confidential and must not be discussed in public

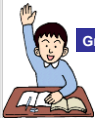
Group-A



Q2

- **Pick the most accurate statement:**
- Cost of Damage from a Cyberattack?**
 - A. Is negligible and most of the times it is not even noticeable.
 - B. May include loss of IP Packets, loss of laptops, or loss of grades in school
 - C. May include loss of reputation, customer trust, human lives and may be even worse compared to the financial loss
 - D. Is reasonable and big companies normally do not care about this loss

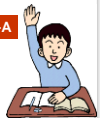
Group-B



Q3

- **Anomaly means:**
 - A. Encrypting the simple information into complicated cipher text
 - B. Listening to confidential conversation
 - C. Launching a Cyber attack by hiring an external hacker
 - D. Deviating from what is standard, normal, or expected trend

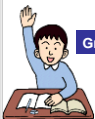
Group-A



Q4

- **Pick the most correct statement**
- **Signature Based Intrusion Detection means**
 - A. Detection of attacks by looking for specific patterns
 - B. Detection of forged signature on a school degree or transcript
 - C. Getting signature from the department head by deceiving him
 - D. Detection of an attack by using surveillance cameras

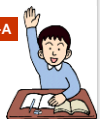
Group-B



Q5

- **Pick the best statement**
- **DPI in terms of cybersecurity stands for**
 - A. Deep Packet Inspection
 - B. Defensive Path Indication
 - C. Deep Pocket Inspection to launch a cyberattack
 - D. Discomfort, Pain and Injury due to cyberattack

Group-A



Q6

- **When an attack happens, it raises several questions such as**
 - A. What information was taken, and who took it, When and how
 - B. Weather we should inform FBI, or should we keep quite
 - C. Weather we should keep using electronic gadgets, or switch back to non digital age and quit using computers
 - D. None of the above



Group-B

Answers to CRQ



Q1

- **Select the best statement**
- **Cost of developing cyber weapons**
 - A. Is almost equal to the cost of developing traditional war weapons
 - B. Is almost negligible compared to the cost of developing traditional war weapons
 - C. Is much higher than the cost of a stealth Bomber
 - D. Is confidential and must not be discussed in public

Group-A

B. Is almost negligible compared to the cost of developing traditional war weapons



Q2

- **Pick the most accurate statement:**
- **Cost of Damage from a Cyberattack?**
 - A. Is negligible and most of the times it is not even noticeable.
 - B. May include loss of IP Packets, loss of laptops, or loss of grades in school
 - C. May include loss of reputation, customer trust, human lives and may be even worse compared to the financial loss
 - D. Is reasonable and big companies normally do not care about this loss

Group-B

C. May include loss of reputation, customer trust, human lives and it might have worse impact compared to the financial loss



Q3

- **Anomaly means:**
 - A. Encrypting the simple information into complicated cipher text
 - B. Listening to confidential conversation
 - C. Launching a Cyber attack by hiring an external hacker
 - D. Deviating from what is standard, normal, or expected trend

Group-A

D. Something that deviates from what is standard, normal, or expected



Q4

- **Pick the most correct statement**
- **Signature Based Intrusion Detection means**
 - A. Detection of attacks by looking for specific patterns
 - B. Detection of forged signature on a school degree or transcript
 - C. Getting signature from the department head by deceiving him
 - D. Detection of an attack by using surveillance cameras

Group-B

A. Detection of attacks by looking for specific patterns



Q5

- Pick the best statement
- DPI in terms of cybersecurity stands for
 - A. Deep Packet Inspection
 - B. Defensive Path Indication
 - C. Deep Pocket Inspection to launch a cyberattack
 - D. Discomfort, Pain and Injury due to cyberattack

Group-A

A. Deep Packet Inspection



Q6

- When an attack happens, it raises several questions such as
 - A. What information was taken, and who took it, When and how
 - B. Whether we should inform FBI, or should we keep quiet
 - C. Whether we should keep using electronic gadgets, or switch back to non digital age and quit using computers
 - D. None of the above

Group-B

A. What information was taken, and who took it, When and how



Homework (10 Points)

Chapter-18 (Due on Next Thursday)

- Questions
 1. What does Anomaly mean in case of Grid Security? What anomalies can be used for threat detection?
 2. What is deep packet inspection?
 3. Intelligent Power system is a cyber physical system that includes hardware, software and physical components. What is the intrusion detection framework for such a system?

No need to
submit this
Homework

Dr. Raziq Yaqub

