

Information Security

CS3002

Lecture 1
19th August 2024

Dr. Rana Asif Rehman
Email: r.asif@lhr.nu.edu.pk

Myself

Dr. Rana Asif Rehman
Associate Professor

Email: **r.asif@lhr.nu.edu.pk**

Phone: (042) 111-128 -128 Ext: 595

Office No. 21, F Block

Department of Cyber Security

FAST School of Computing, FAST-NUCES, Lahore.

Aim of the course

This course serves as a comprehensive overview to the field of information security at senior undergraduate level.

At the end of the course the students will be able to:

1. Explain key concepts of information security such as design principles, cryptography, risk management, and ethics
2. Discuss legal, ethical, and professional issues in information security
3. Apply various security and risk management tools for achieving information security and privacy
4. Identify appropriate techniques to tackle and solve problems in the discipline of information security

Books and Resources

- Cryptography and Network Security: Principals and Practice by William Stallings, Edition 7th
- Principle of Information Security by Whitman & Mattord, Edition 6
- Computer Security: Principals and Practice by William Stallings, Edition 4th

Course contents

- Introduction to Information Security
- Security design principles
- Security mechanisms including symmetric and asymmetric cryptography, encryption, hash functions, digital signatures
- Key management, authentication and access control
- Software security, vulnerabilities and protections
- Malware
- Database security
- Network security
- Firewalls
- Intrusion detection
- Web Security
- Security policies, policy formation and enforcement

Marks Distribution



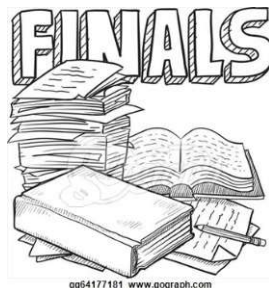
Quizzes 10%

Assignments/Labs 10%



Project 10%

Midterm 25-30%



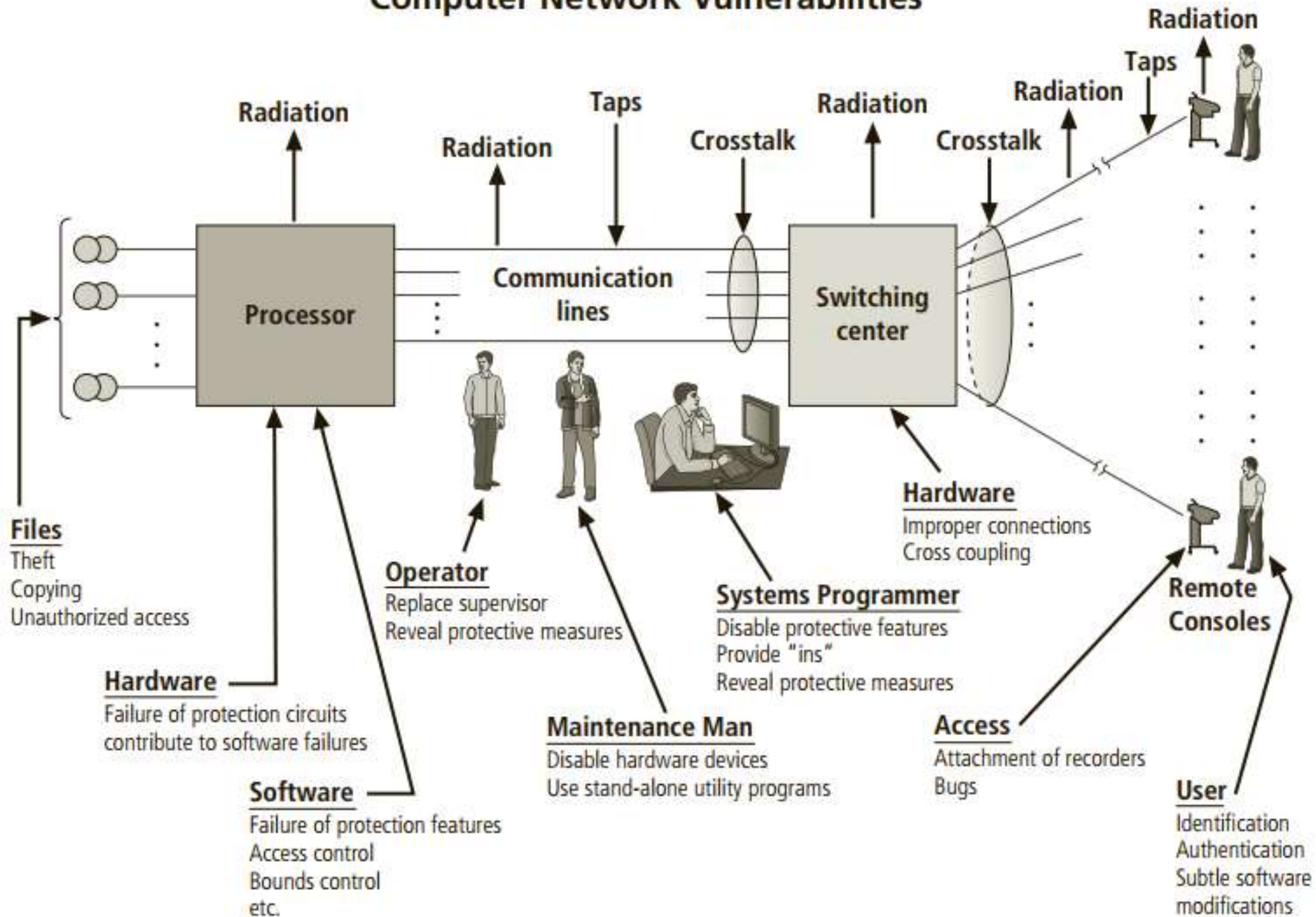
40-45%

Class Rules & Regulations

- **Quizzes**
 - All quizzes will be **Announced**
 - Quizzes will have more weightage as compared to Assignments
- **Assignments**
 - In case of copied, all remaining assignment will be marked **Zero**
 - Avoid late submission, **No** assignment will be entertained after deadline
 - Don't send me assignments by using email, submit them on Google Class
 - Assignments **Viva** will also be conducted (during semester)
- **Attendance**
 - Don't mark Proxy of your friend (If he/she is your real friend 😊)
 - In case of proxy, **5 Absents** will be marked to that student
 - In case of emergency, get permission personally or send an email prior to the class
 - Attend all classes regularly, no attendance issue will be entertained in the end of semester

Are you ready !!!!
Lets Begin

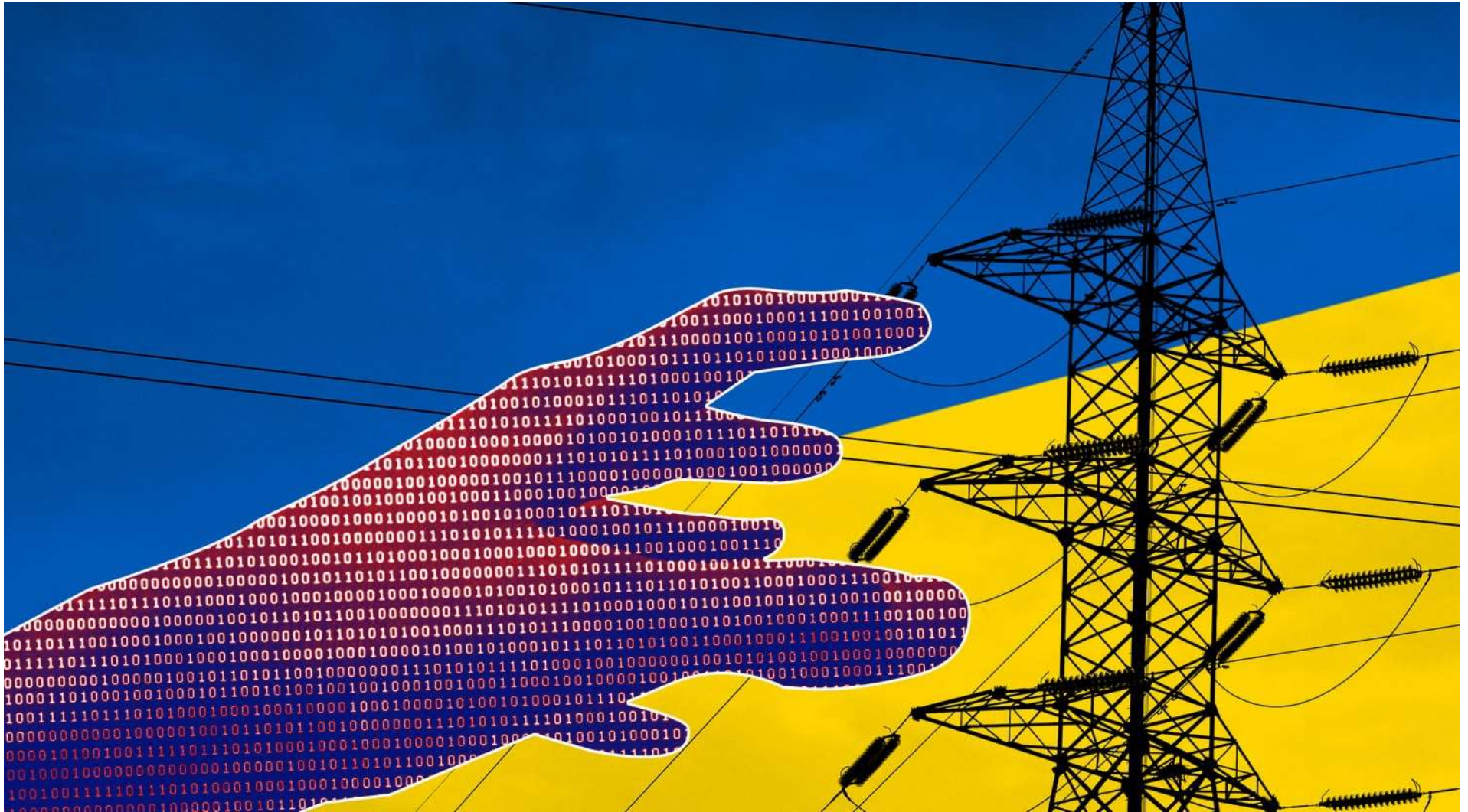
Computer Network Vulnerabilities



What is Security?

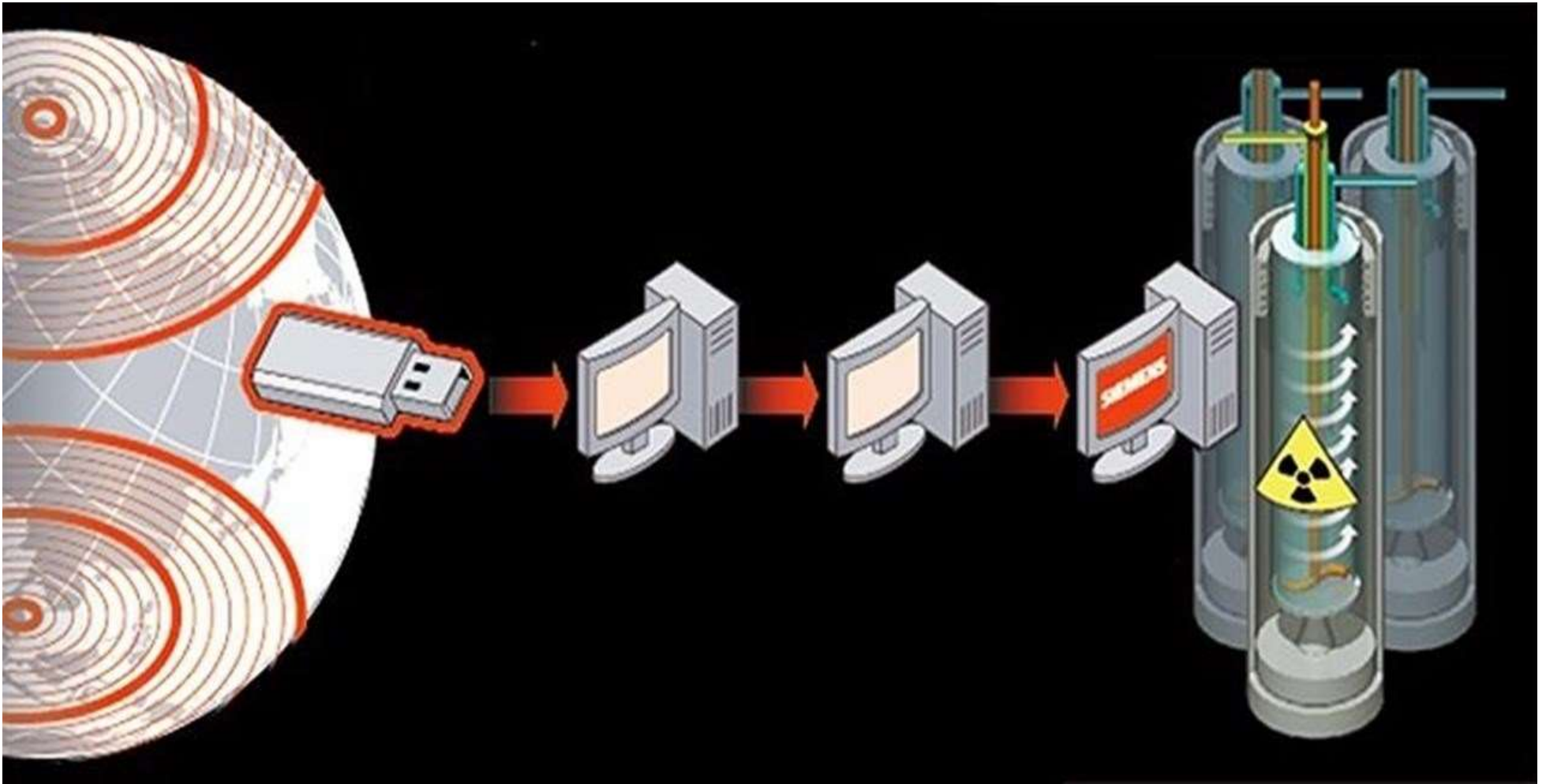
- “The quality or state of being secure—to be free from danger”
- A well secured organization should have multiple layers of security in place:
 - Physical security
 - Personal security
 - Operations security
 - Communications security
 - Network security

Real World Example:



Ukraine Power Grid Attack (2015)

Real World Example:




Stuxnet (2010)

Real World Example:

Pakistani banks hit by biggest cyber attack in country's history

Data of 19,864 cards from 22 banks dumped for sale on the dark web

SAMAA | Farooq Baloch and Iftikhar Firdous - Posted: Nov 6, 2018 | Last Updated: 2 years ago

 Pakistani banks hit by biggest cyber attack in country's history

Data of 19,864 cards from 22 banks dumped for sale on the dark web

DAWN

TODAY'S PAPER | DECEMBER 06, 2020

K-Electric struck by 'ransomware'

Sumaira Jajja | Updated 10 Sep 2020

KARACHI: K-Electric on Wednesday said it experienced an attempted cyber-incident earlier this week. "The KE teams have initiated consultation with international information security experts and are also collaborating with local authorities in this regard," the company said in a statement.

The admission came days after customers across the city complained that they were unable to lodge power outage and technical fault complaints using 118 helpline, 8119 SMS service and KE Live App or check the company's website for duplicate bills.

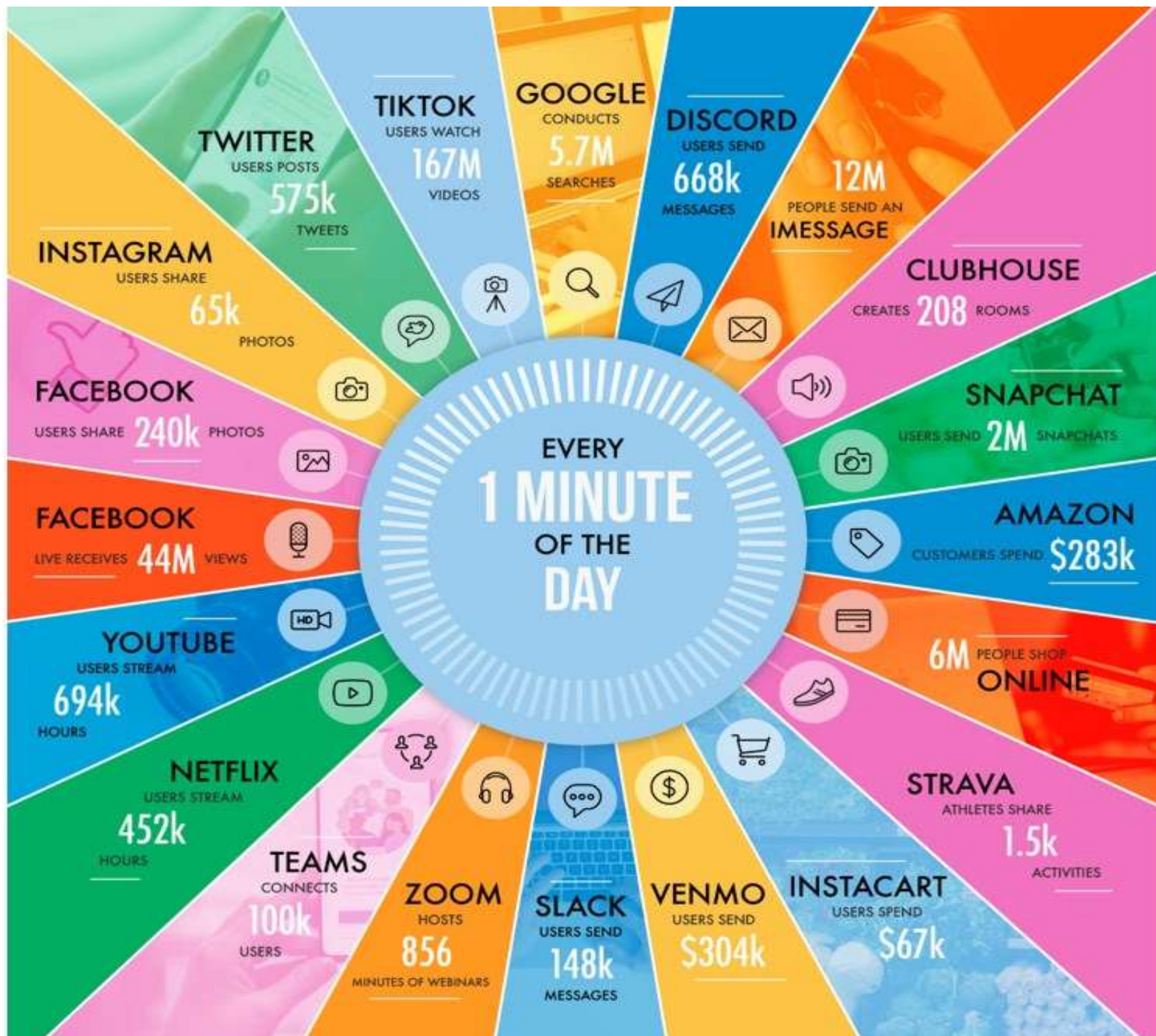
On Tuesday, KE had issued a statement telling customers to expect disruptions to some online services but made no mention of the "cyber-incident".

NATIONAL September 25, 2022

Leaked conversations of PM, minister put up for sale on darknet

By Staff Report

Why?



Digital Footprint: Be careful



Information Security



- The protection of information and its critical elements, including systems and hardware that use, store, and transmit that information
- Necessary tools: policy, awareness, training, education, technology
- C.I.A. triangle was standard based on confidentiality, integrity, and availability
- C.I.A. triangle now expanded into list of critical characteristics of information

Critical Characteristics of Information

- The value of information comes from the characteristics it possesses:
 - Timeliness
 - No value if it is too late
 - Availability
 - No interference or obstruction
 - Required format
 - Accuracy
 - Free from mistakes
 - Authenticity
 - Quality or state of being genuine, i.e., sender of an email

Critical Characteristics of Information

- Confidentiality
 - Disclosure or exposure to unauthorized individuals or system is prevented
- Integrity
 - Whole, completed, uncorrupted
 - Cornerstone
 - Size of the file, hash values, error-correcting codes, retransmission
- Possession
 - Ownership
 - Breach of confidentiality results in the breach of possession

Components of an Information System



Source: shapecharge

People



Source: 4X-image

Hardware



Source: Ali Kerem Yucael

Software



Source: Ovcinnikov Vladimir

Networks



Source: NAN104

Data



Source: Pinkypills

Components of an Information System



Source: Mark Agnor

Procedures

Components of an Information System

- **Information System (IS)** is entire set of software, hardware, data, people, procedures, and networks necessary to use information as a resource in the organization
- **Software**
 - Perhaps most difficult to secure
 - Easy target
 - Exploitation substantial portion of attacks on information
- **Hardware**
 - Physical security policies
 - Securing physical location important
 - Laptops
 - Flash memory

Components of an Information System

- Data
 - Often most valuable asset
 - Main target of intentional attacks
- People
 - Weakest link
 - Social engineering
 - Must be well trained and informed
- Procedures
 - Threat to integrity of data
- Networks
 - Locks and keys won't work