

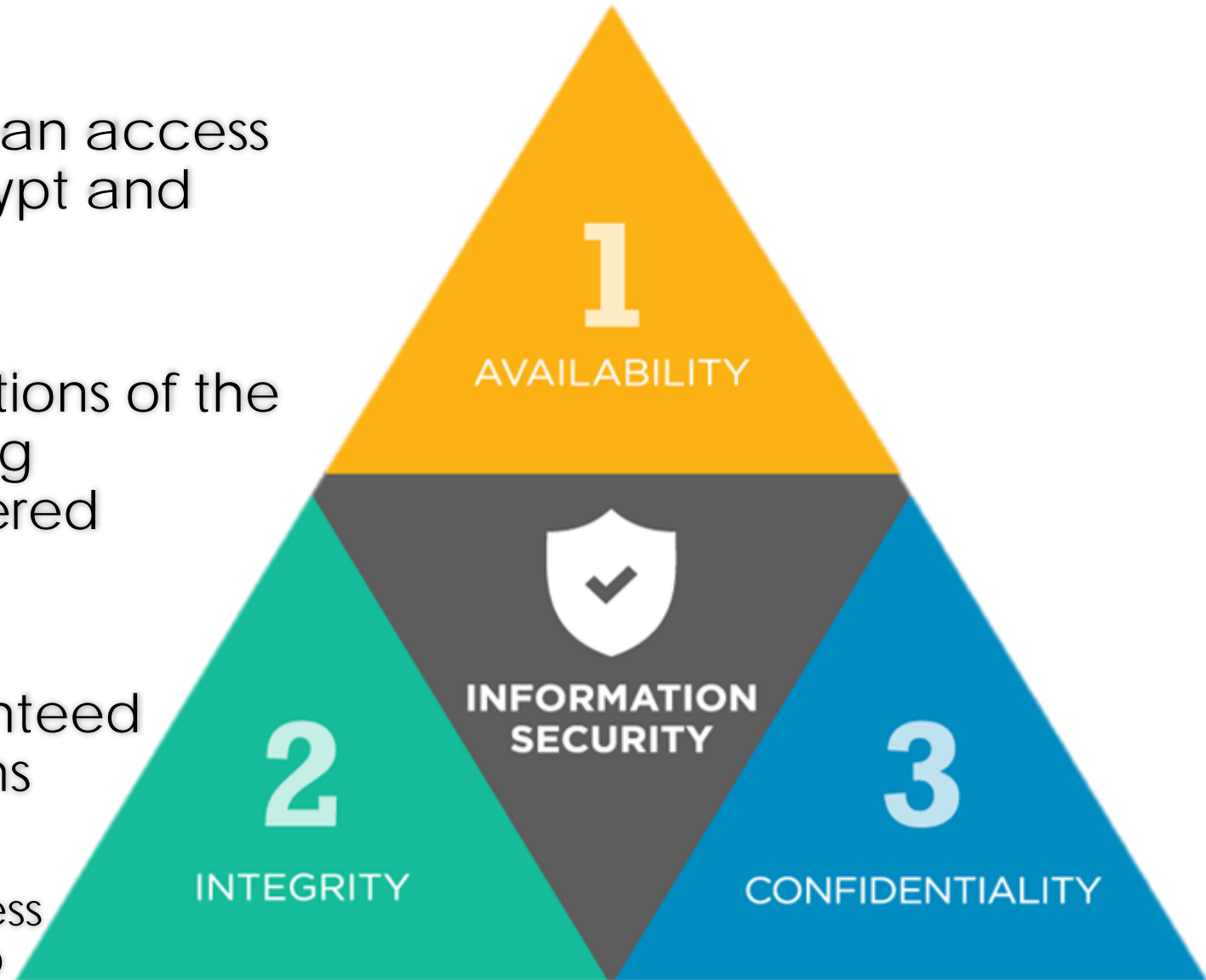
CIA

Confidentiality, Integrity and Availability

Dr. Shahzada Khurram

CIA

- **Confidentiality:**
We ensure no one unauthorized can access the data. Uses encryption to encrypt and hide data.
- **Integrity:**
How we protect against modifications of the data and the systems .Uses hashing algorithms to ensure data is unaltered during operation.
- **Availability:**
Assures data is accessible. Guaranteed by network hardening mechanisms and backup systems.
We ensure authorized people can access the data they need, when they need to



Confidentiality

○ We use:

- ✓ Encryption for **data at rest** (for instance AES256), full disk encryption.
- ✓ Secure transport protocols for **data in motion**. (SSL, TLS or IPSEC).
- ✓ Best practices for **data in use** - clean desk, no shoulder surfing, screen view angle protector, PC locking (automatic and when leaving).
- ✓ Strong passwords, multi factor authentication, masking, access control, need-to- know, least privilege.

○ Threats:

- Attacks on your encryption (cryptanalysis).
- Social engineering.
- Key loggers (software/hardware), cameras, Steganography.
- IOT (Internet Of Things) – The growing number of connected devices we have pose a new threat, they can be a backdoor to other systems.

○ Threats

- Capturing network traffic
- Unauthorized access to network
- Password dump stealing
- Social engineering
- Port scanning
- Eavesdropping

○ Countermeasures

- Encryption
- Authentication to systems
- Access control
- Data classification
- End-user training

Integrity

○ We use:

- ❑ Cryptography (again).
- ❑ Check sums (This could be CRC).
- ❑ Message Digests also known as a hash (This could be MD5, SHA1 or SHA2).
- ❑ Digital Signatures – non-repudiation.
- ❑ Access control.

○ Threats:

- Alterations of our data.
- Code injections.
- Attacks on your encryption (cryptanalysis).

○ Threats

- Virus
- Logic bombs
- Errors
- Malicious modifications
- Intentional replacement
- System back door

○ Countermeasures

- Activity logging
- Access control
- Authentication
- Hashing
- Encryption
- Intrusion detection systems

Availability

○ We use:

- ❑ IPS/IDS.
- ❑ Patch Management.
- ❑ Redundancy on hardware power (Multiple power supplies/UPS), Disks (RAID), Traffic paths (Network design), HVAC, staff, HA (high availability) and much more.
- ❑ SLA's – How high uptime to we want (99.9%?) – (ROI)

○ Threats:

- Malicious attacks (DDOS, physical, staff).
- Application failures (errors in the code).
- Component failure (Hardware).

○ Threats

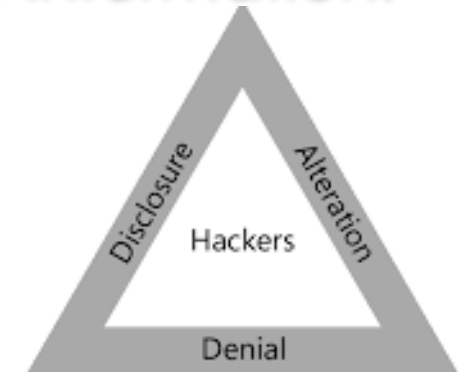
- Device failure
- Software error
- Natural calamity
- Power
- Human error
- oversight

○ Countermeasures

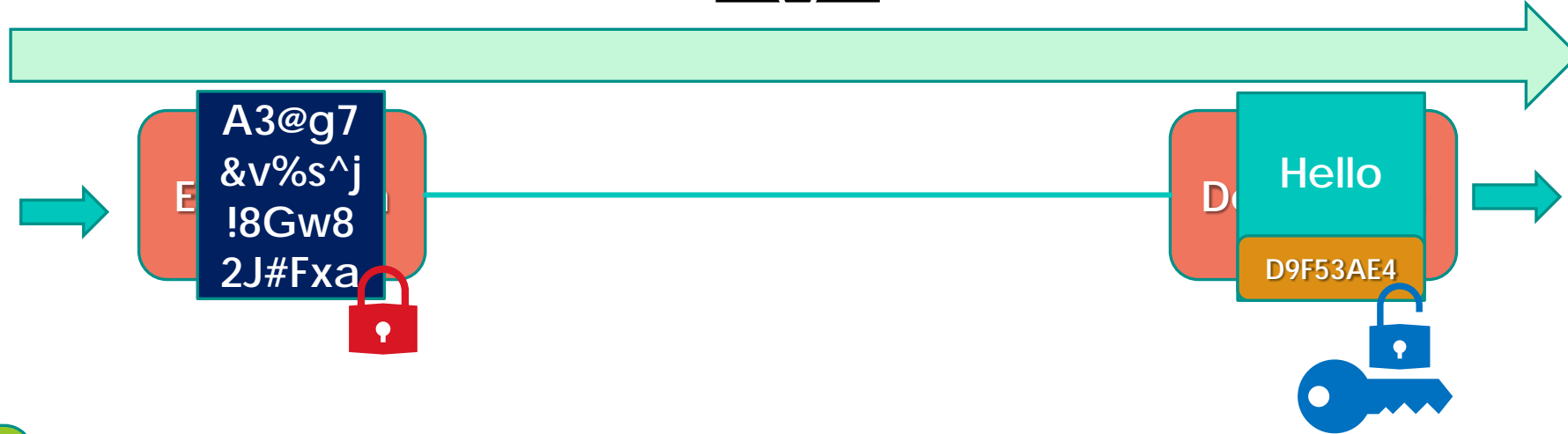
- RAID
- Redundant systems
- Clustering
- Access control
- BCP/DRP
- Fault tolerance

CIA and DAD

- Finding **the right mix** of Confidentiality, Integrity and Availability is a balancing act.
- This is really the cornerstone of IT Security – finding the RIGHT mix for your organization.
 - Too much Confidentiality and the Availability can suffer.
 - Too much Integrity and the Availability can suffer.
 - Too much Availability and both the Confidentiality and Integrity can suffer.
- The opposites of the CIA Triad is **DAD** (Disclosure, Alteration and Destruction).
 - ❖ **Disclosure** – Someone not authorized getting access to your information.
 - ❖ **Alteration** – Your data has been changed.
 - ❖ **Destruction** – Your data or systems have been destroyed or rendered inaccessible.

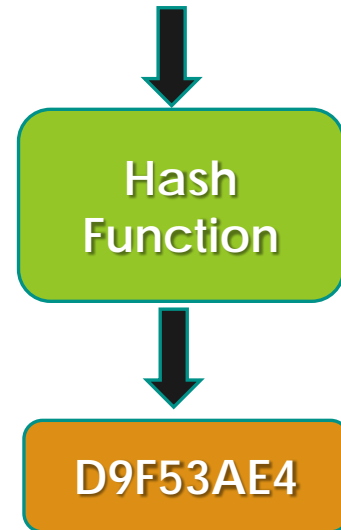
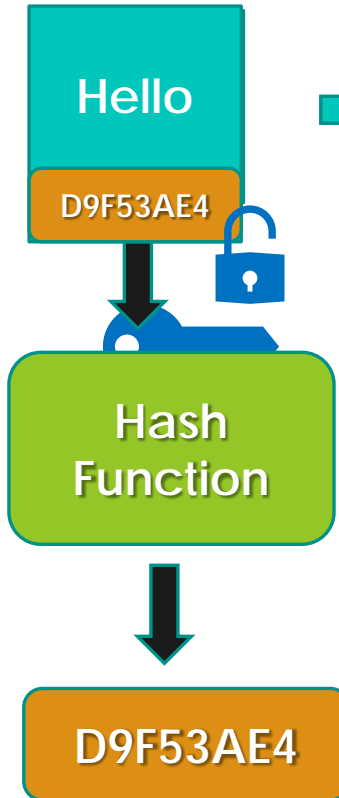


CIA



Ahyan wants to send the "Hello" Message to Hibba

But there is an intruder



Match



Thank you