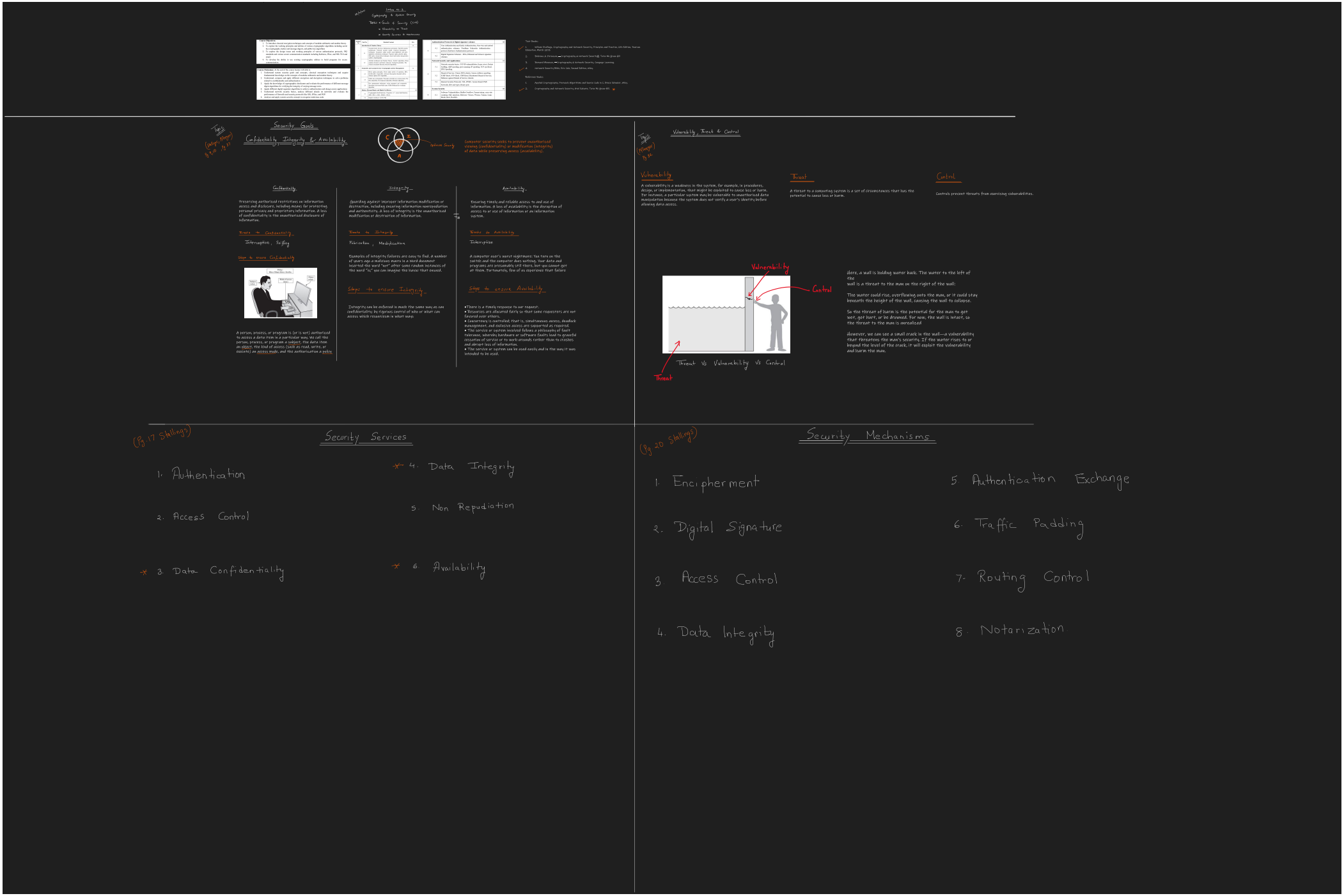
Security Goals
Confidentiality Integrity & Availability
Computer security seeks to prevent unauthorized viewing (confidentiality) or modification (integrity) of data while preserves access (availability).
Confidentiality
Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information.
Integrity
Guarding against improper information modification or destruction, including ensuring information nonrepudiation and authenticity. A loss of integrity is the unauthorized modification or destruction of information.
Availability
Ensuring timely and reliable access to and use of information. A loss of availability is the disruption of access to or use of information or an information system.
Vulnerability, Threat & Control
Vulnerability
A vulnerability is a weakness in the system, for example, in procedures, design, or implementation, that might be exploited to cause loss or harm. For instance, a particular system may be vulnerable to unauthorized data manipulation because the system does not verify a user's identity before allowing data access.
Threat
A threat to a computing system is a set of circumstances that has the potential to cause loss or harm.
Control
Controls prevent threats from exercising vulnerabilities.
Vulnerability
Control
Threat
Threat Vs Vulnerability Vs Control
Here, a wall is holding water back. The water to the left of the wall is a threat to the man on the right of the wall:
The water could rise, overflowing onto the man, or it could seep beneath the height of the wall, causing the wall to collapse.
So the threat of harm is the potential for the man to get wet, get hurt, or be drowned. For now, the wall is intact, so the threat to the man is unrealized
However, we can see a small crack in the wall—a vulnerability that threatens the man's security. If the water rises to or beyond the level of the crack, it will exploit the vulnerability and harm the man.
Security Services
1. Authentication
2. Access Control
3. Data Confidentiality
4. Data Integrity
5. Non Repudiation
6. Availability
Security Mechanisms
1. Encipherment
2. Digital Signature
3. Access Control
4. Data Integrity
5. Authentication Exchange
6. Traffic Padding
7. Routing Control
8. Notarization