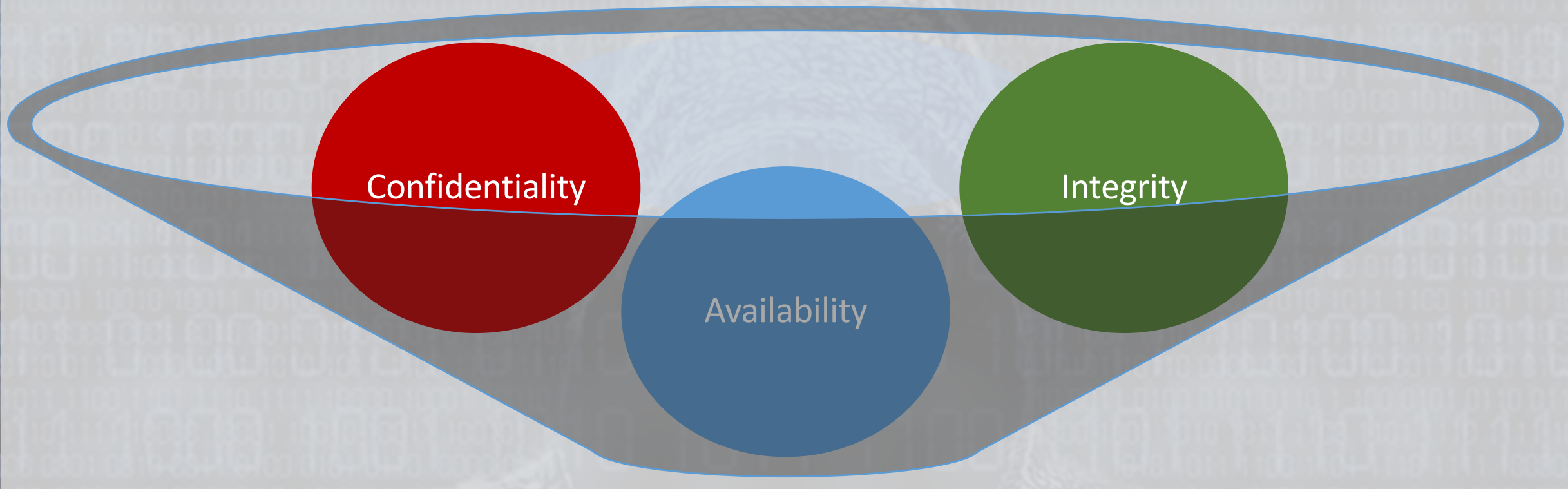
# The CIA Triad

*(…and we aren't talking about intelligence)*

# Components of the Security (CIA) Triad




Information Systems Security,
Data and Services

# Confidentiality

- How secure is the information?
- How secure does the data need to be?

- Physical Protections
  - Locked doors, fences, security guards, security cameras, safes, …
- Electronic Protections
  - Encryption (storage and in transit), passwords, firewalls, two-factor authentication, …

- Failure of confidentiality occurs if someone can obtain and view the data

# Integrity

- How correct is the information?
- Has the data been modified during retrieval, in transit, or in storage?
- Hashing of files and information
- Checksums during data transmission
- Failure of integrity occurs if someone modifies the data being stored in or transit

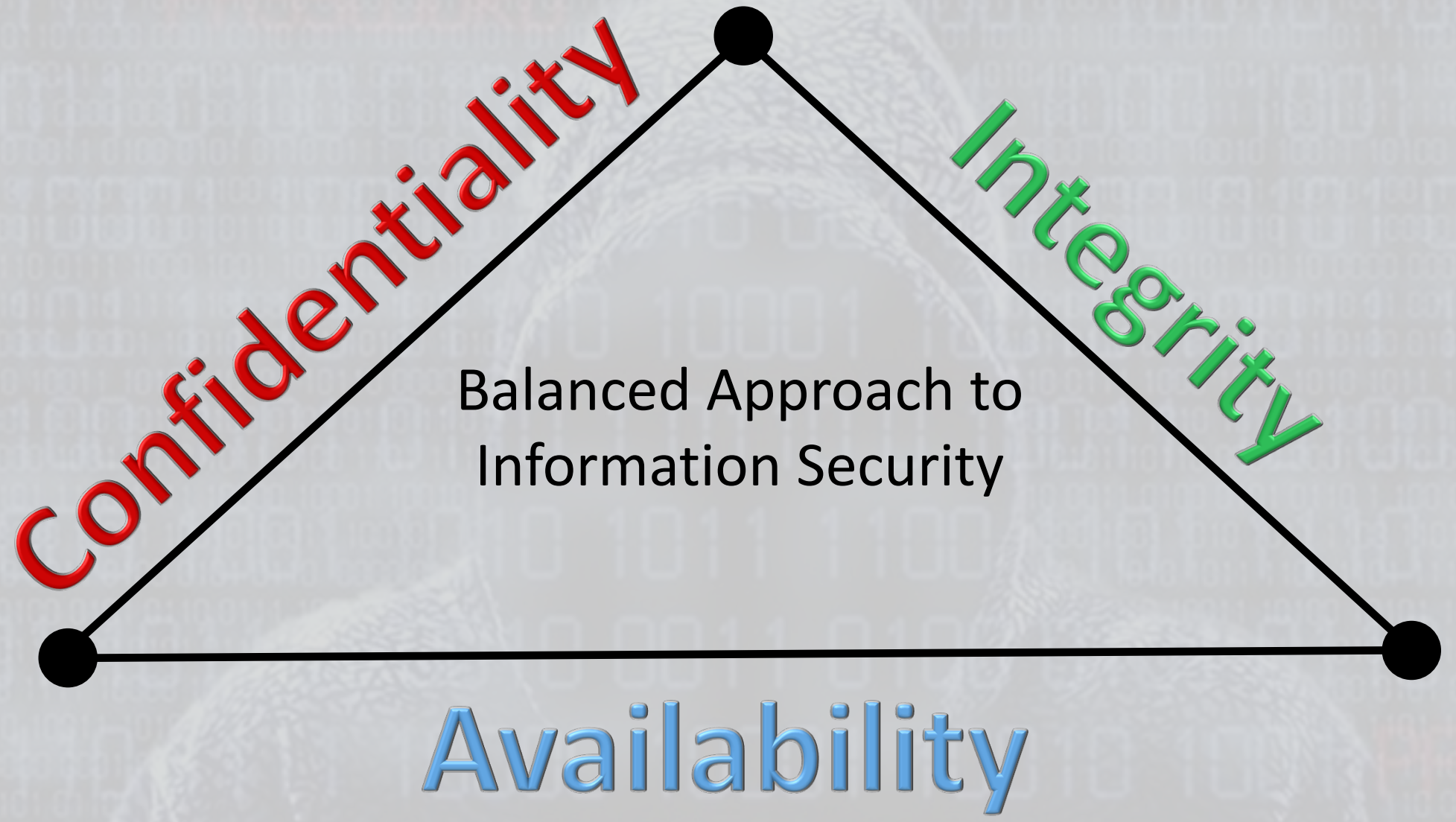
=

```
79054025
255fb1a2
6e4bc422
aef54eb4
```

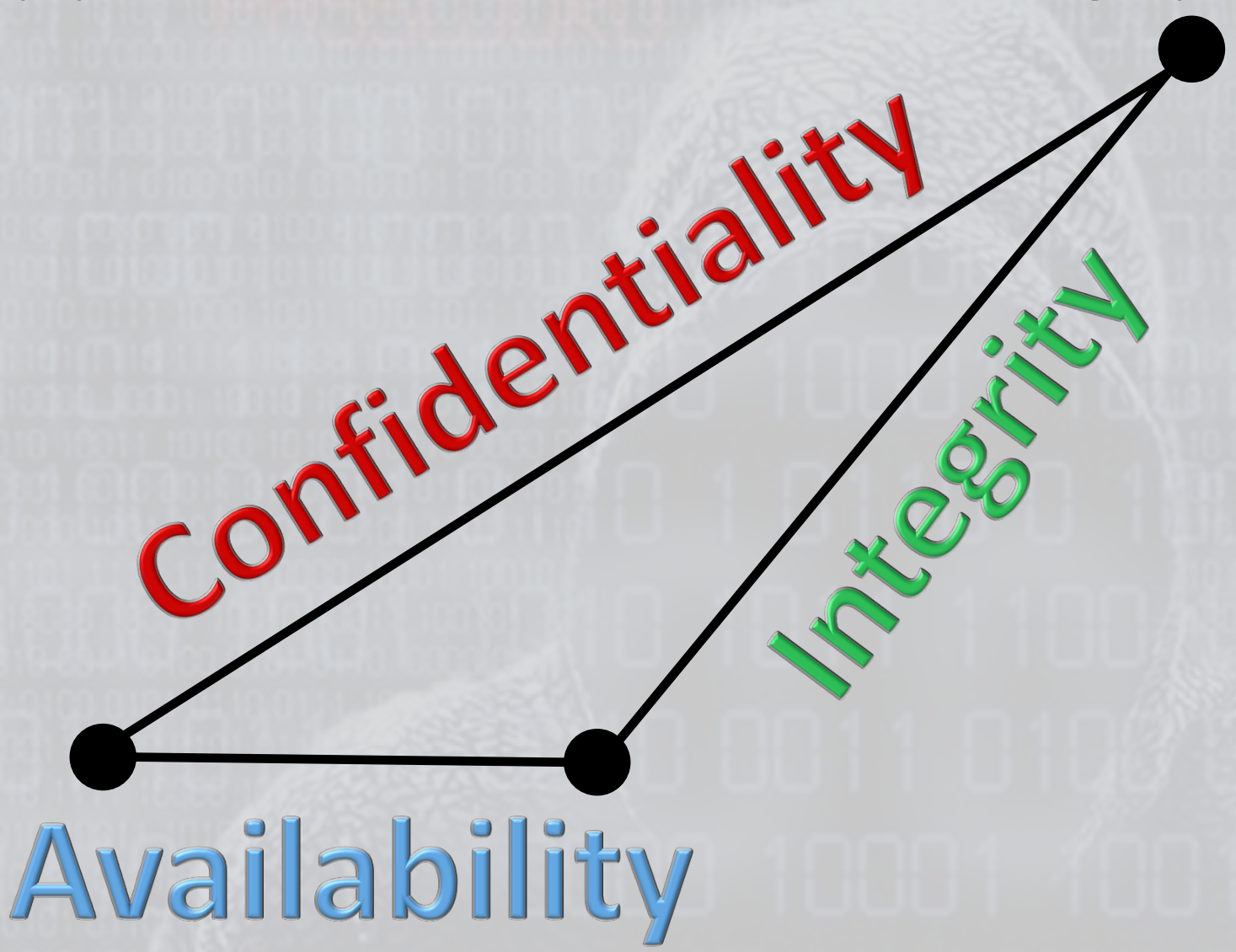
# Availability

- How much uptime is the system providing?
- Is the data accessible by users at all times?
- Redundancy in the system design, including components and data paths
- Backup strategies and disaster recovery plan
- Failure of availability occurs if the data cannot be accessed by the end user

# Approaches to the Security (CIA) Triad



# Approaches to the Security (CIA) Triad

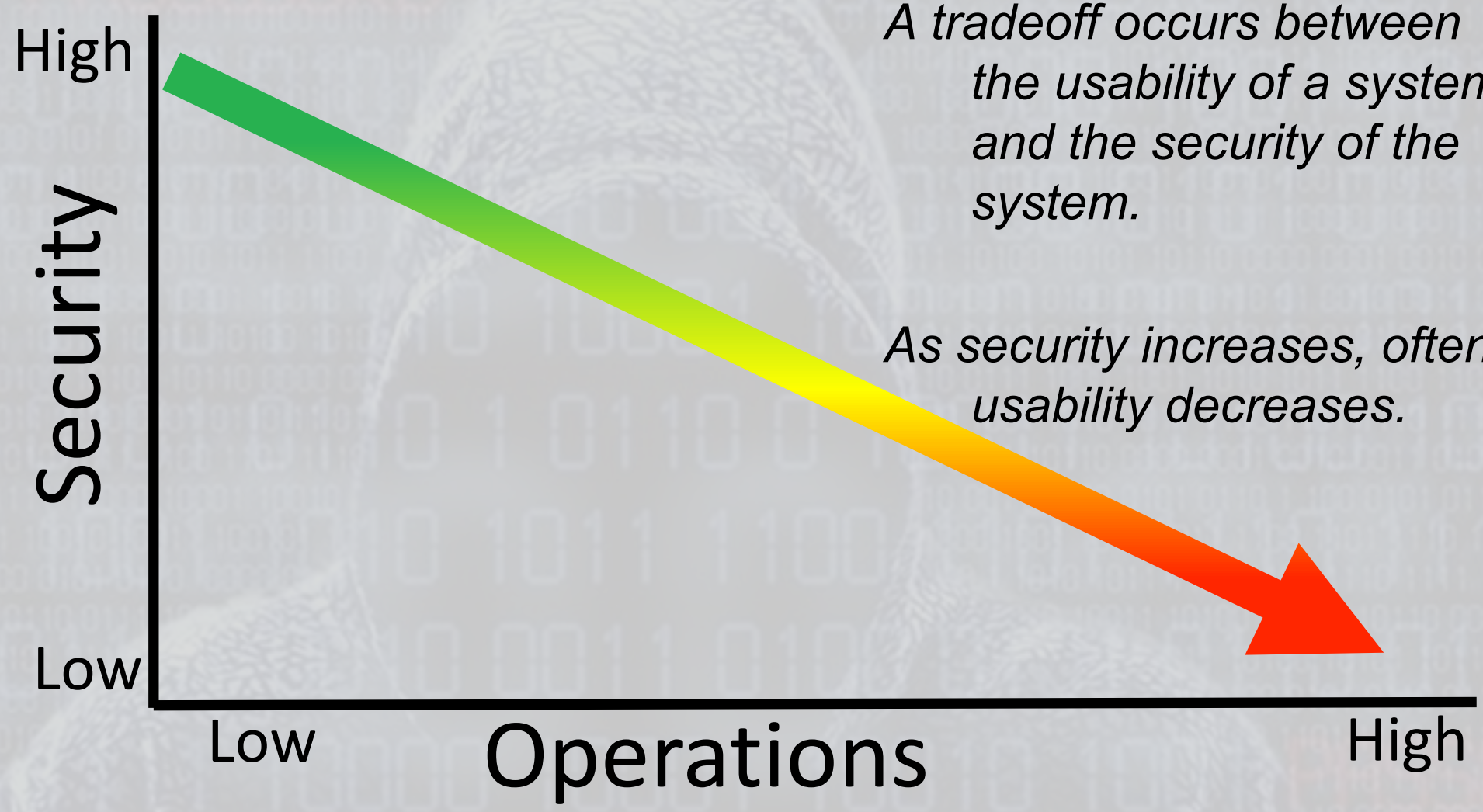



High Confidentiality
High Integrity
Low Availability

# Approaches to the Security (CIA) Triad

Low Confidentiality
High Integrity
High Availability

# Security vs Operations




*A tradeoff occurs between the usability of a system and the security of the system.*

*As security increases, often usability decreases.*

# The CIA Triad

*(…and we aren't talking about intelligence)*