Secure Software Development Requirements

Objectives

- Differentiate between security goals and security functions
- Explain the concept of a security requirement
- List the three characteristics for secure software
- Explain the concept of a security profile
- Explain confidentiality requirements
- Explain integrity requirements
- Explain authentication requirements
- Compare and contract simple authentication, two factor authentication, and multifactor identification

How do you describe a system

Use cases / UML

Architecture
⇒ Nothing guessing

Functionality
⇒ Features & Functions

How do you describe a system

Normalitive Behavior
⇒ correct usage assumed
⇒ Assumed defect free.

Assumptions
No one will abuse the system ... No bad guys.

- What makes for good requirements?

Focus on what system does what it Works properly.
⇒ Unambiguous
⇒ Complete
⋮

Requirements

MSOE

- What is the key difference between software quality and software security?

Conceptualization

Malicious Intent

What security requirements are NOT

- Security goals

Abstract statements, which may conflict w/ each other

- Security functions

⇒ encryption part of solution

⇒ May Lead to non-optimal designs/incomplete designs

Secure Software Characterization

- Reliability
  - The software functions as it is expected to
- Resiliency
  - The software does not violate any security policy and is able to withstand the actions of threat agents that are posed intentionally
- Recoverability
  - The software is able to restore operations to what the business expects by containing and limiting damage

What security is not

- Not a component that can be added to software
  - Cryptography
  - SSL
  - 128 bit encryption
- The tent example

only works if it is used right

Security Requirements

- Definition
  - Security requirements represent constraints placed upon functional requirements to achieve security goals
- Typically define what the system shall not do.
  - Example:
    - The system shall not provide Personnel Information except to members of the Human Resources Department.

Question

- Which of the following policies is most likely to include the following requirement? "All software processing financial transactions needs to use more than one factor to verify the entity requesting access."

a. Authorization

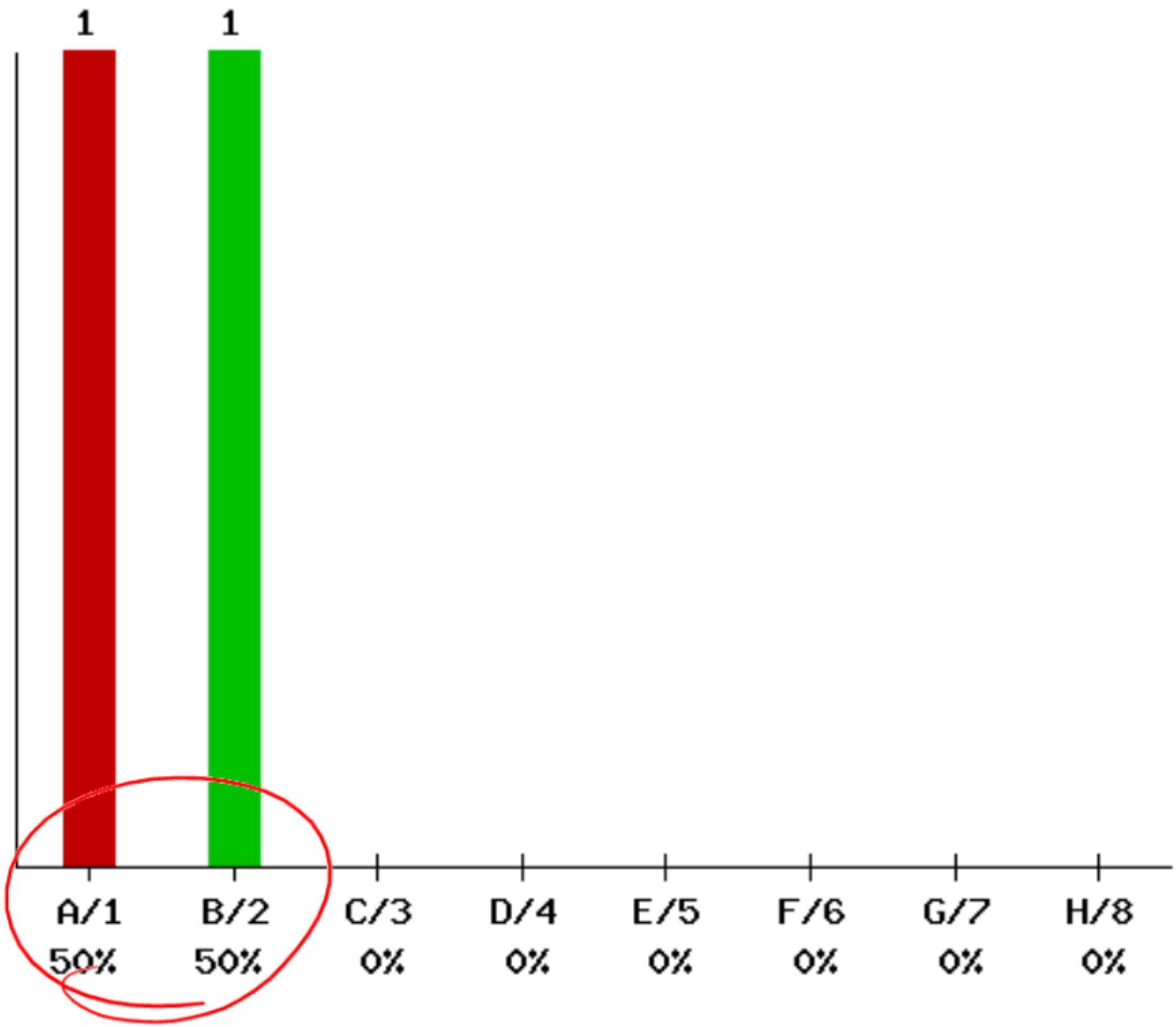
b. Authentication

c. Auditing

d. Availability

e. Resiliency

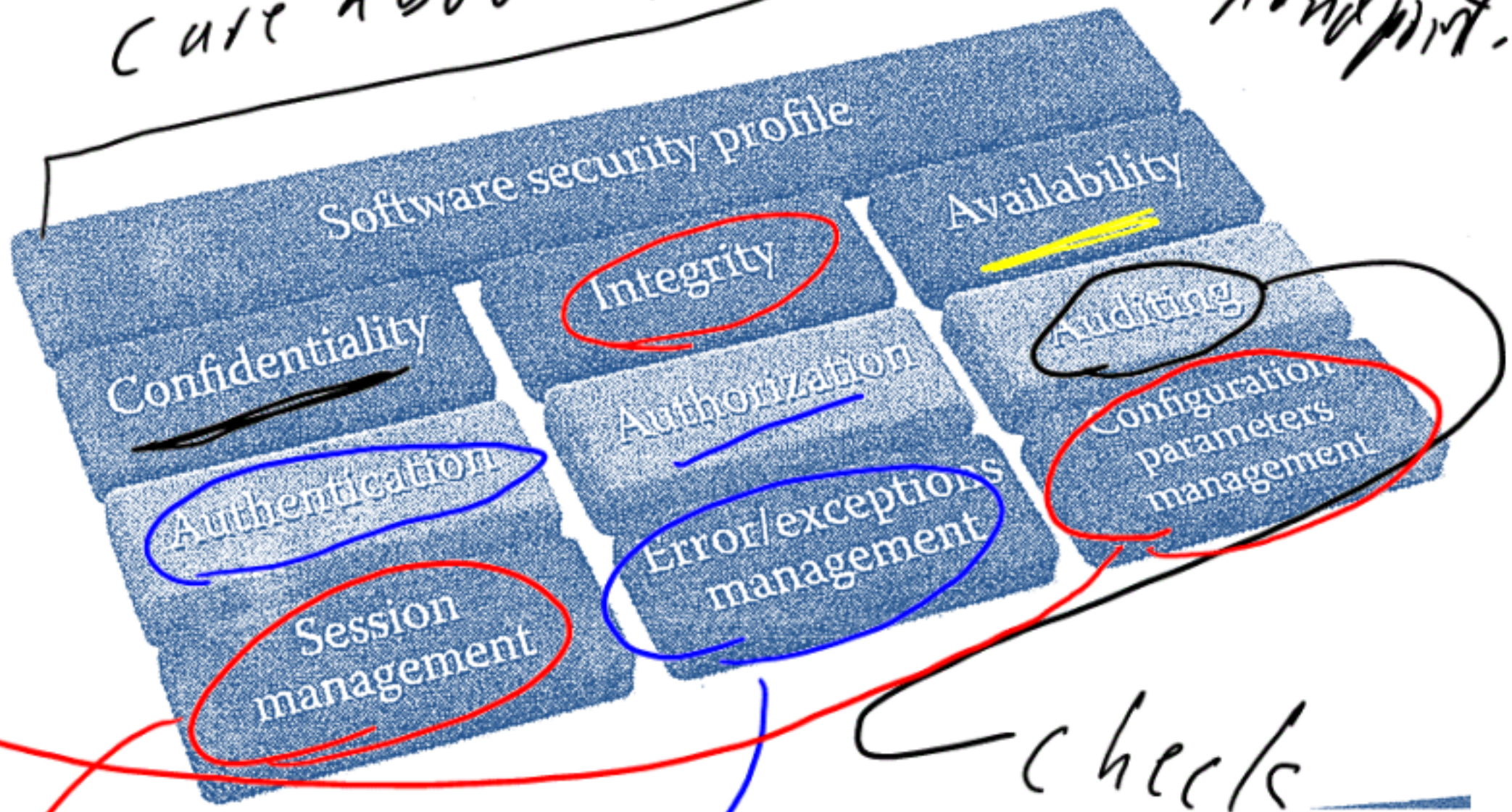
Authentication is that a user is who they say they are


1
1
A/1
B/2
C/3
D/4
E/5
F/6
G/7
H/8
50%
50%
0%
0%
0%
0%
0%
0%

Software Security Profile

How do we setup our SW?

Defines what we care about from a security standpoint.



Connections

when things go wrong?

check

what happens

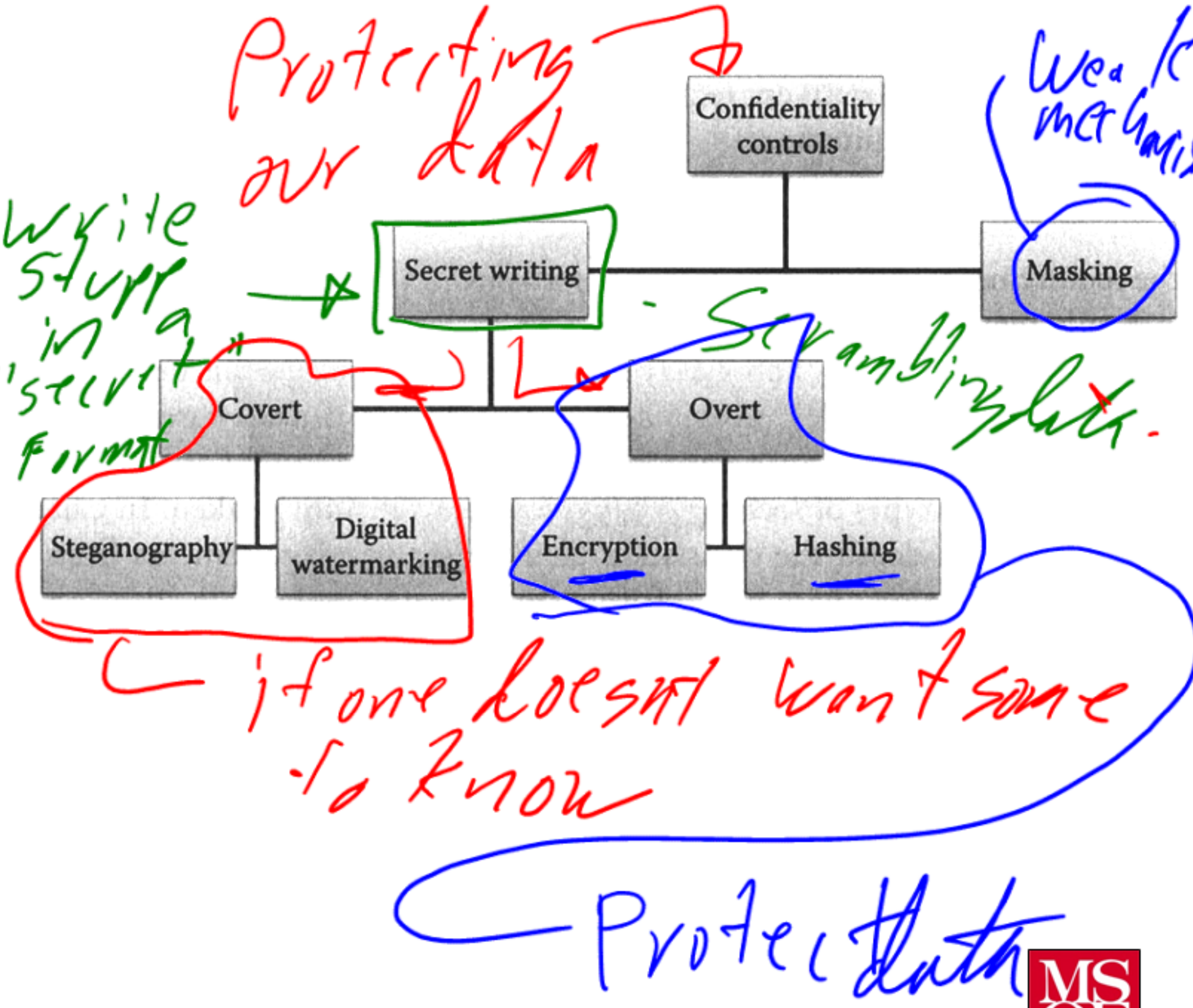
Taxonomy of Security Requirements

Security requirements			
Software security profile	Confidentiality	Integrity	Availability
	Authentication	Authorization	Auditing
	Session management	Error/ exceptions management	Configuration parameters management
Other	Sequencing and timing	Archiving	International
	Deployment environment	Procurement	Antipiracy

Confidentiality Requirements

- Requirements that address protection against the disclosure of data or information that is either personal or sensitive in nature
  - Uses data classification to define
  - Accomplished by one of many techniques
  - Need to be defined throughout the information lifecycle, from the origin of the data until retirement

Confidentiality Protection Mechanisms



Example confidentiality requirements

- Personal health information must be protected against disclosure using approved encryption mechanisms
- Passwords and other sensitive input fields need to be masked
- The use of nonsecure transport protocols such as File Transfer Protocol (FTP) to transmit account credentials in clear to third parties outside of your organization shall not be allowed.

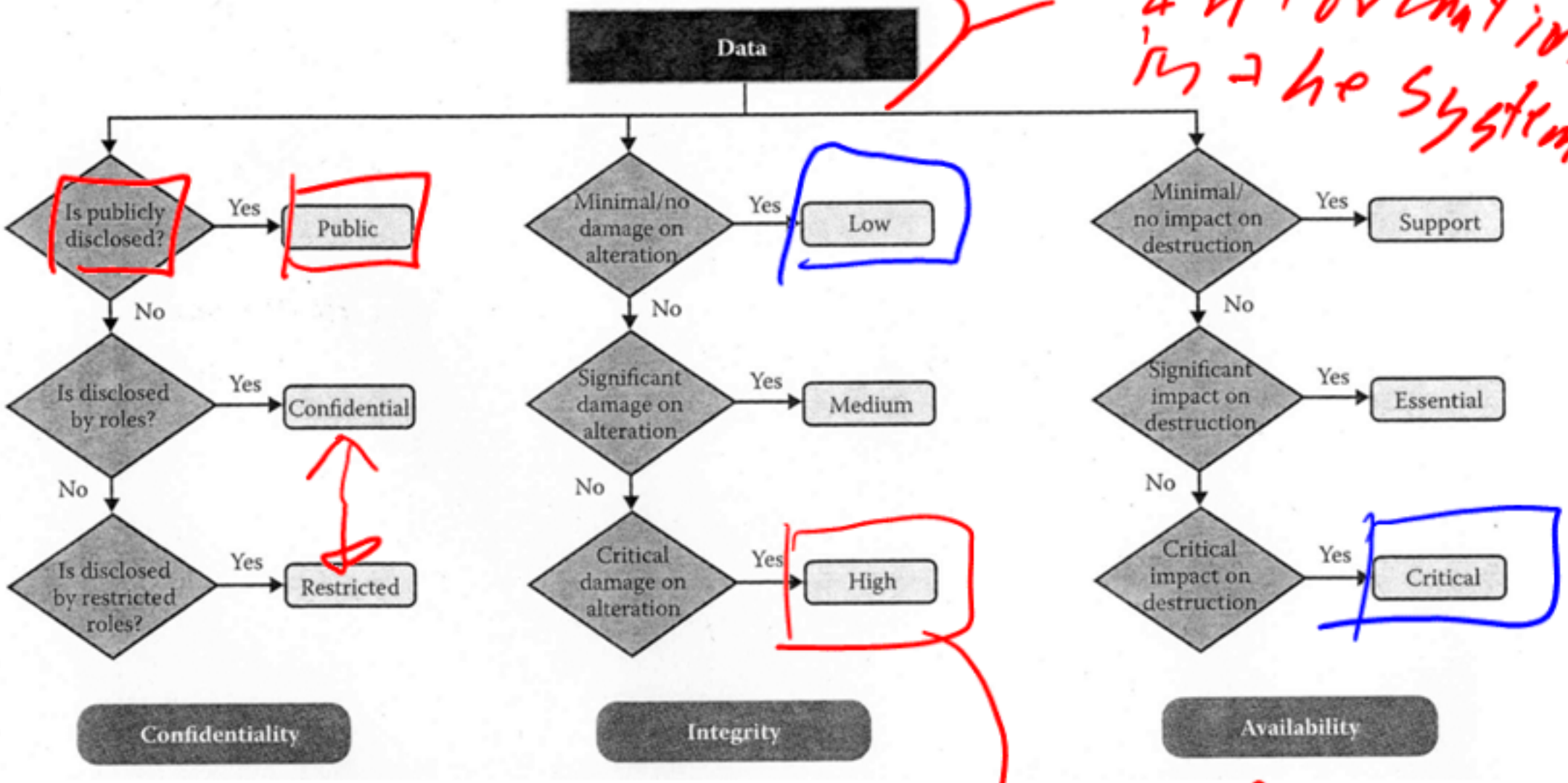
Integrity Requirements

- Address reliability assurance and protection against unwanted modification
  - Needs to deal with both system and data integrity
- May use one or more of the following
  - Input validation
  - Parity bit checking
  - hashing

Example Requirements

- All input forms and query strings shall be validated against a set of allowable inputs before the software accepts it for processing
- All messages transmitted over the internet shall be checked for corruption before being processed

Categorization of data

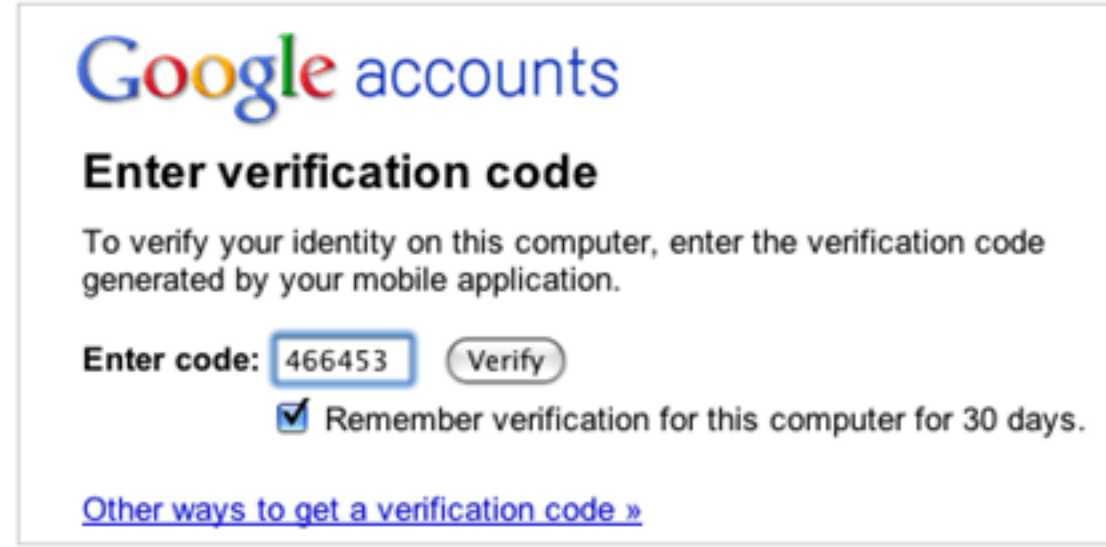


Authentication requirements

- The process of validating an entity's claim
  - Are you who you say you are
- Two factor identification
  - Uses two factors for identification
  - Something someone knows
  - Something someone has

1.

2.



- Multifactor authentication
  - Uses multiple factors for authentication