Introduction to Cyber security and profession ethics

CSEC1310

Security overview

Agenda

- What is security
- Information security vs Cyber Security
- CIA triad
- The Parkerian hexad
- Types of attack
- Threats, Vulnerabilities, Assets(impact),risk
- Risk management and Risk mitigation
- Defense in depth

What security is about in general?

- “Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction,” according to US law .In essence, it means we want to protect our data (wherever it is) and systems assets from those who would seek to misuse it.”
- According to Gollman security is about protection an assets

Security phases

- Prevention
  - take measures that prevent your assets from being damaged (or stolen)
- Detection
  - take measures so that you can detect when, how, and by whom an asset has been damaged
- Reaction
  - take measures so that you can recover your assets

Real world example

- Prevention
  - locks at doors, window bars, secure the walls around the property, hire a guard
- Detection
  - missing items, system alarms, closed circuit TV
- Reaction
  - call the police, replace stolen items, make an insurance claim

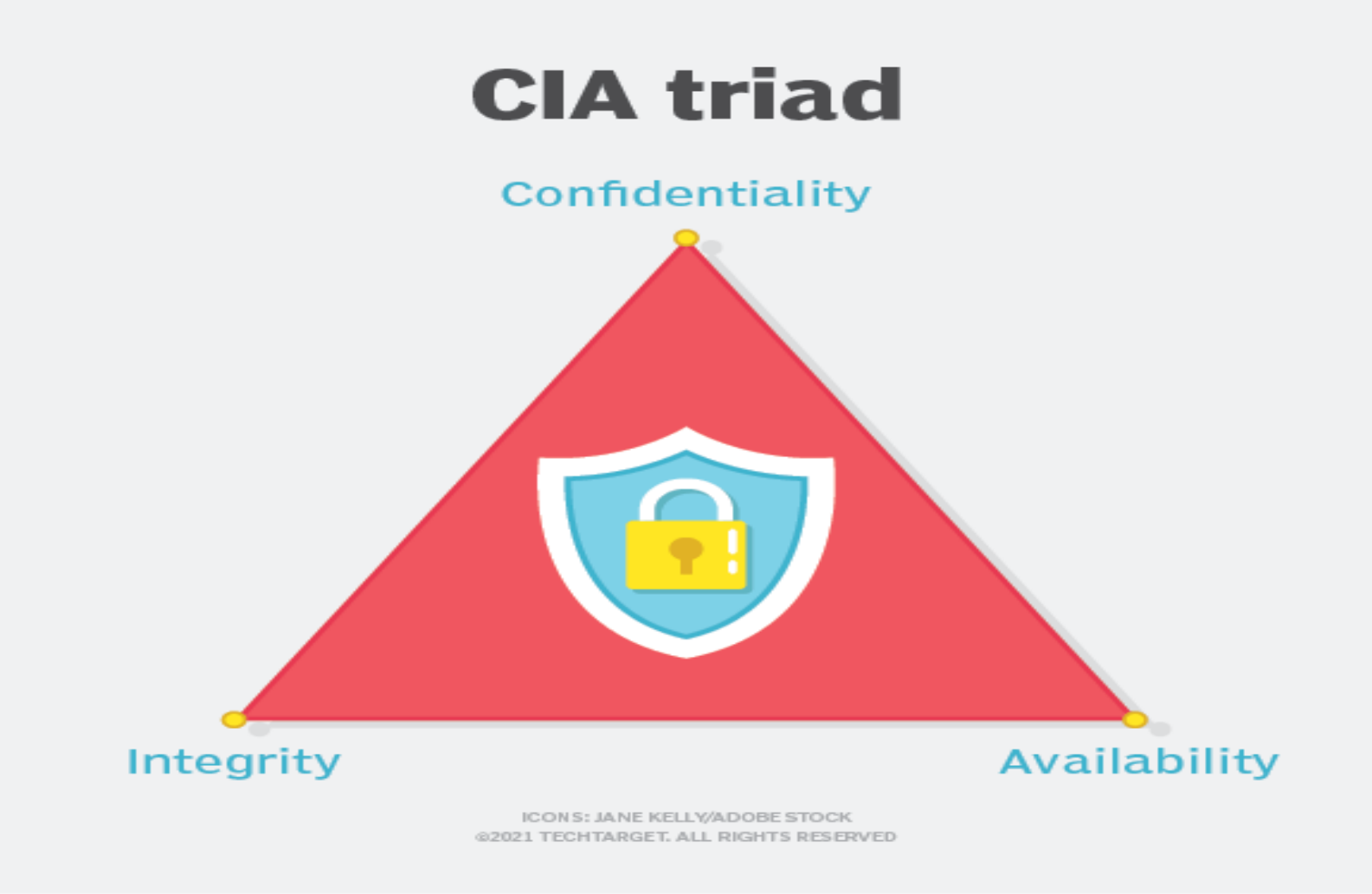
Internet shopping example

- Prevention
  - encrypt your order and card number, enforce merchants to do some extra checks, don't send card number via Internet
- Detection
  - an unauthorized transaction appears on your credit card statement
- Reaction
  - complain, dispute, ask for a new card number, sue (if you can find of course ☺)
  - Or, pay and forget (a glass of cold water) ☺

Information security vs Cyber security

- Protecting within the cyber scope
- Yes there are many diffrence but at least in this course we are not going to highlight those diffrences
- Cyber security is a subset of information security.
- Cybersecurity focuses entirely on computer and web-related security. In contrast, information security covers all forms of securing information. Cybersecurity is a type of information security.

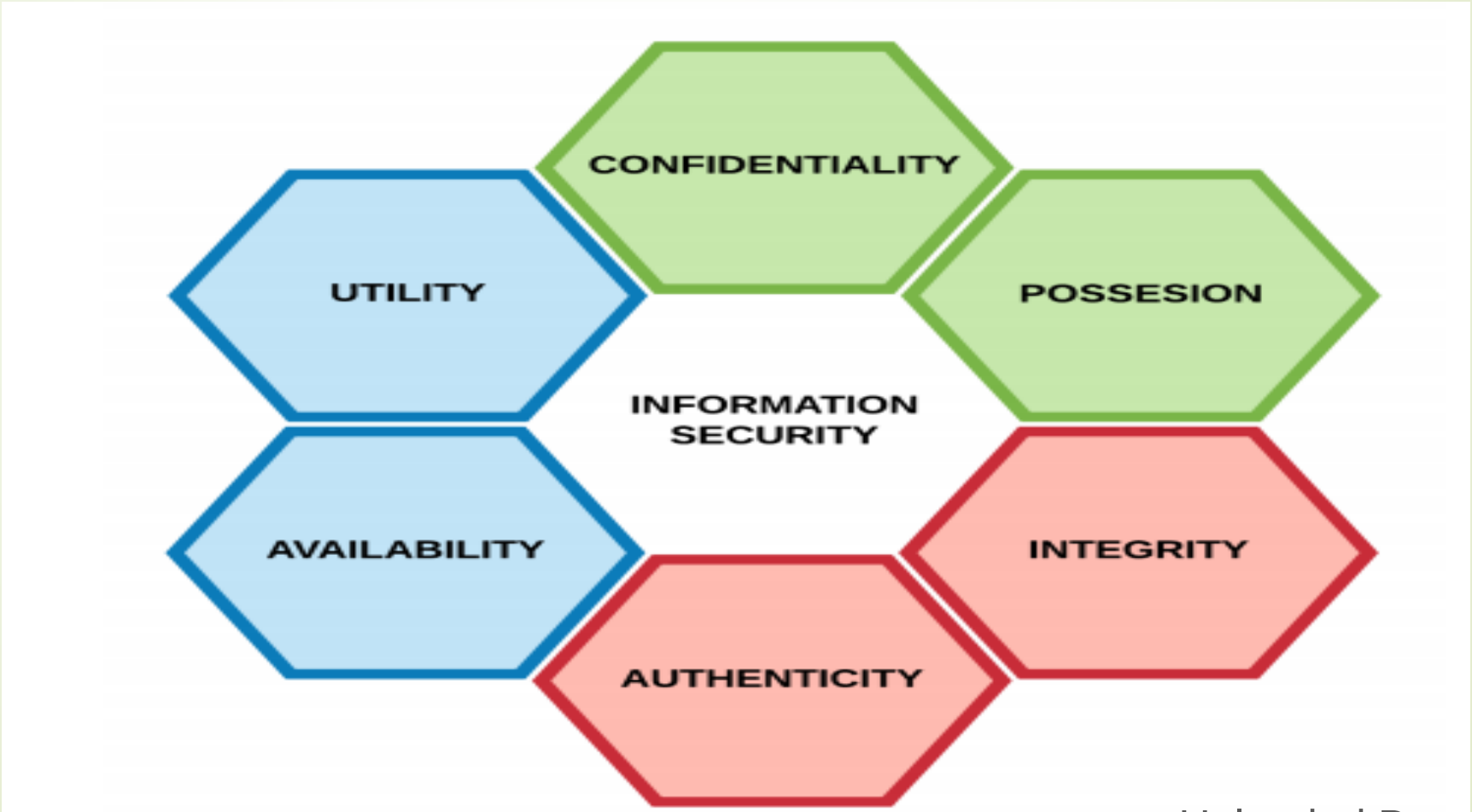
CIA triad -1



CIA-triad - 2

- Confidentiality: prevent unauthorized disclosure of information
- Integrity: prevent unauthorized modification of information
- Availability: prevent unauthorized withholding of information or resources

Parkerian hexad-1



Parkerian hexad-2

- Authenticity: know whom you are talking to

- Possession: the physical disposition of the media on which the data is stored .

  Assuring the control of physical media that contains data.

- Utility: how useful the data is to us .

  measurement of usefulness.

Attack

- A basic definition is exploiting a vulnerability in a system attach a specific threat to a vulnerability.
- A lot of scenarios
- Social engineering .
- Identity theft.
- Denial of service.
- Uncountable .

Classifications and Motivations

- Organized crime to gain Money.
- Terrorists (critical infrastructure).
- Governments.(inside and outside)
- The competition.(commercial)
- Hacktivists: This class of attackers tries to break into your systems to make a political point or demonstrate regarding social issues(political)
- For fun
- Attacker Skill Levels: From Script Kiddies to the Elite

Threat

- An action by an attacker who try to exploit vulnerabilities to damage the assets.
  - Spoofing identity.
  - Tampering data.
  - Gain a privilege.
  - Denial of service.
  - Repudiation.
  - Disclosure.

Asset

- A property in an enterprise
  - Hardware
  - Software
  - Data and information
  - Reputation.

Vulnerability

- A Weakness attached to an Asset
- Accounts with a privileges where the default password for ”Manager” has not been changed.
- Programs with known flows or unnecessary privileges.
- Weak access control.
- Weak firewall configurations.
- How much is critical.????(admin than guest).

Risk Management and Risk mitigation

- The possibility that an attack cause damage to your enterprise.
  - Risk = Assets ×Threats ×Vulnerabilities.
- To have a quantitive values are taken from mathematical domain (asset replacement, probability of threat.)
- Qualitative we will mention some principles later

Defense in depth (Layers)