SWINBURNE UNIVERSITY OF TECHNOLOGY

Theory of Blockchain

Session 1:

Fundamental Security Concepts

Module 3 – Terminology of the Security Domain

Key Terms in the Security Domain

- **Vulnerability**

  A weakness in the design, implementation or operation of a system

- **Threat**

  The possibility/potential that an adversary takes advantage of the vulnerability

- **Attack**

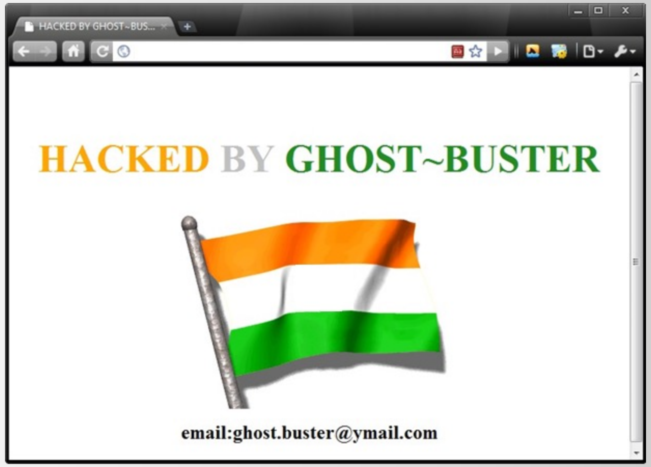
  Act of exploiting a vulnerability

Key Terms

- **Asset:**

  Every valuable thing owned. Examples are:

  - Devices, Tools, Machinery, …
  - Valuable information / data / plans
  - Bandwidth
  - Employees (people)
  - Reputation -> Website defacing attacks target this
  - …



HACKED BY GHOST~BUSTER

email:ghost.buster@ymail.com

Key Terms (cont'd)

- **Incident:**

  A set of events that once triggered, jeopardize the security.

  notice that not all events are incidents!

- **Risk**

  A measure for assessing an uncertain source's impact on objectives/assets.

Key Terms

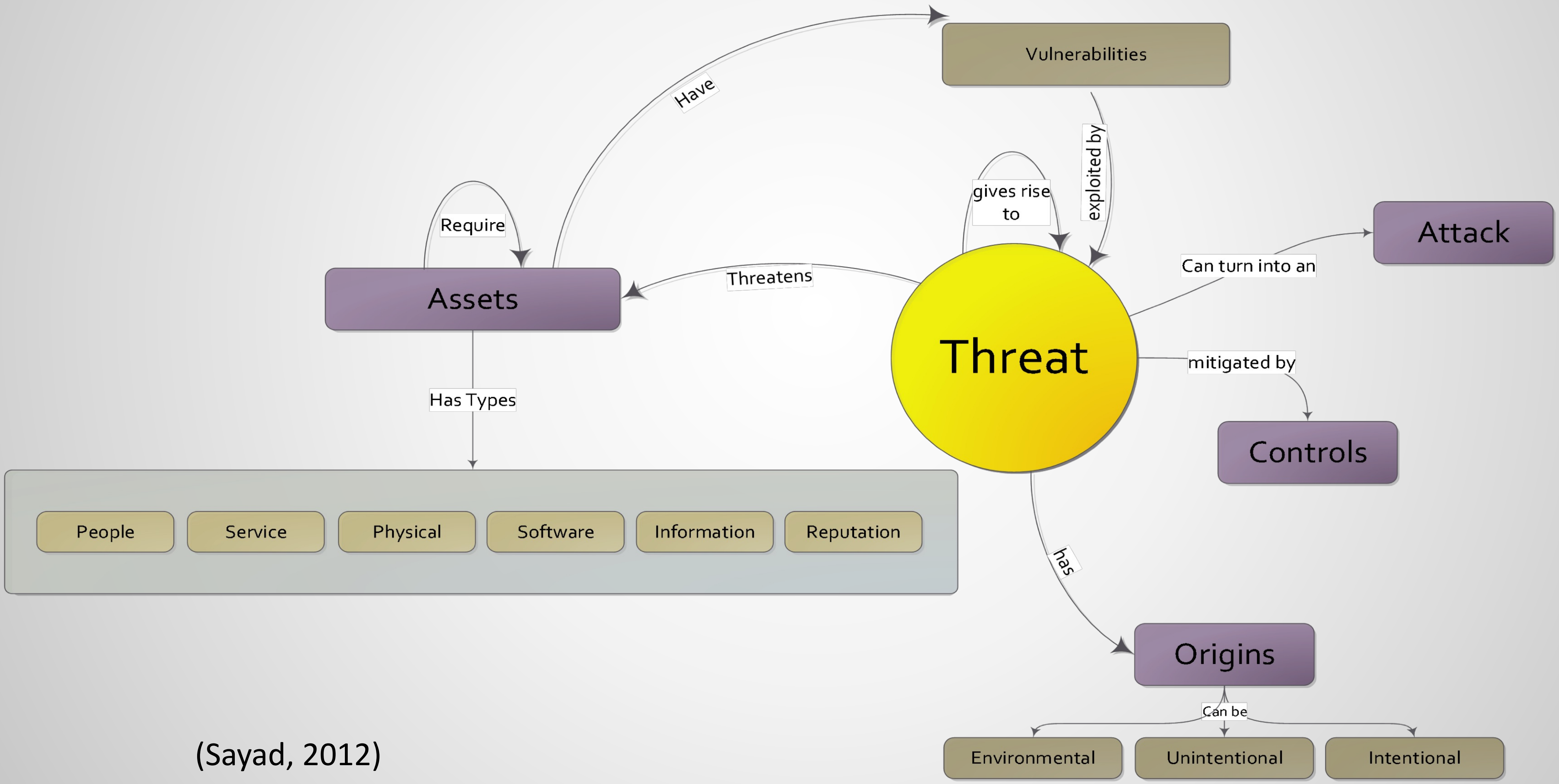
- **Control:**

  Every technical, legal or administrative method used to manage and reduce the risk. Examples:

  - Trainings
  - Policies
  - Procedures
  - Security Cameras
  - Antiviruses
  - Firewalls
  - …

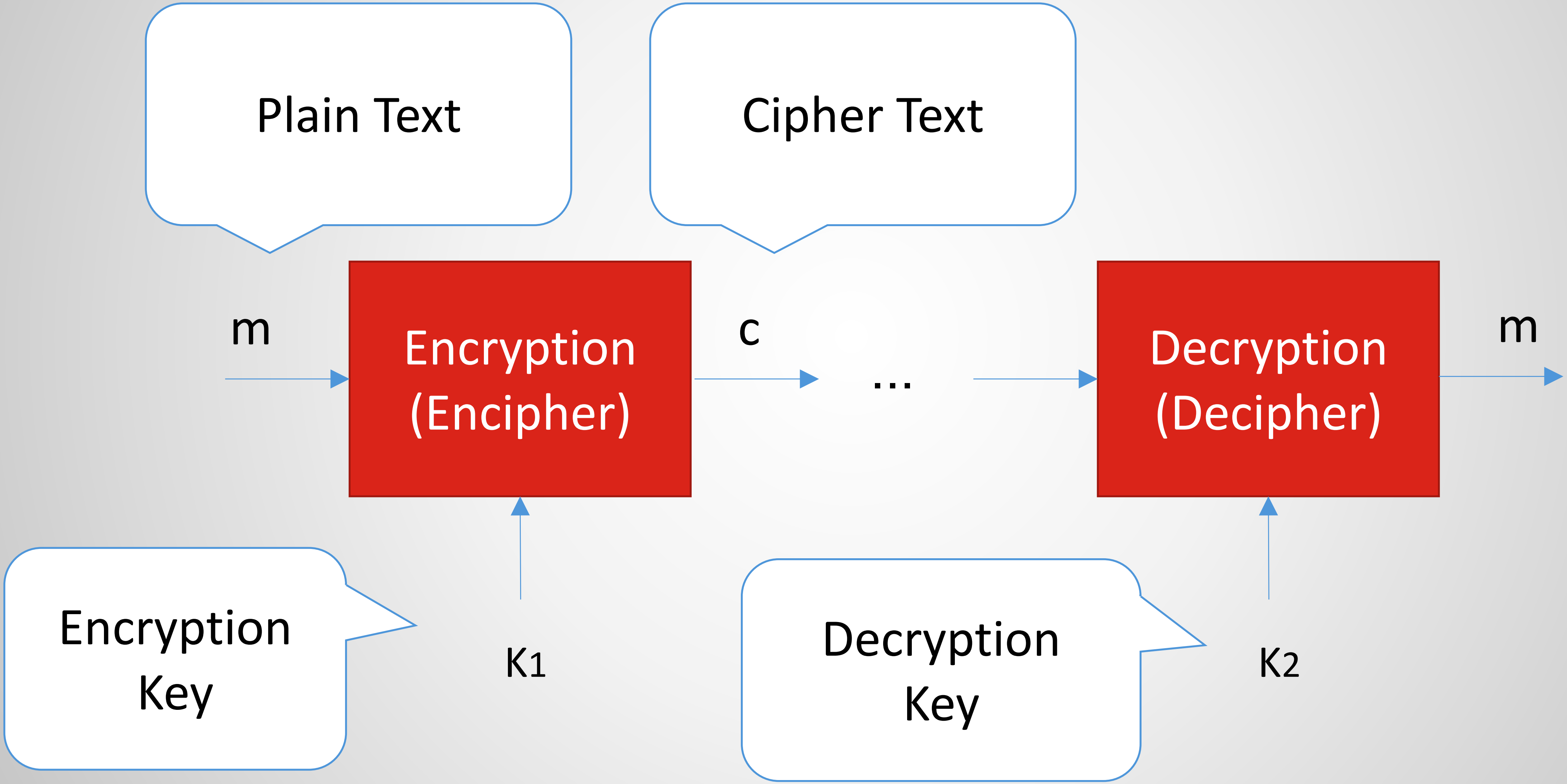
- **Cryptanalysis**
  - An analysis aiming at breaking a cyptosystem, mainly targeting the key. Has 2 types.
    - cryptanalytic attack
    - brute-force attack

Key Definitions/Terms Relationships



(Sayad, 2012)

Terminology in Cryptography



What Comes Next …

- We learned about technical terms in security and cryptography and how to interpret them.

- In the next video, we will learn some cryptographic primitives as well as symmetric ciphers and see their applications.

See you in the next video …