Threats and Security goals

Hyoungshick Kim

Department of Software

College of Software

Sungkyunkwan University

Common threats

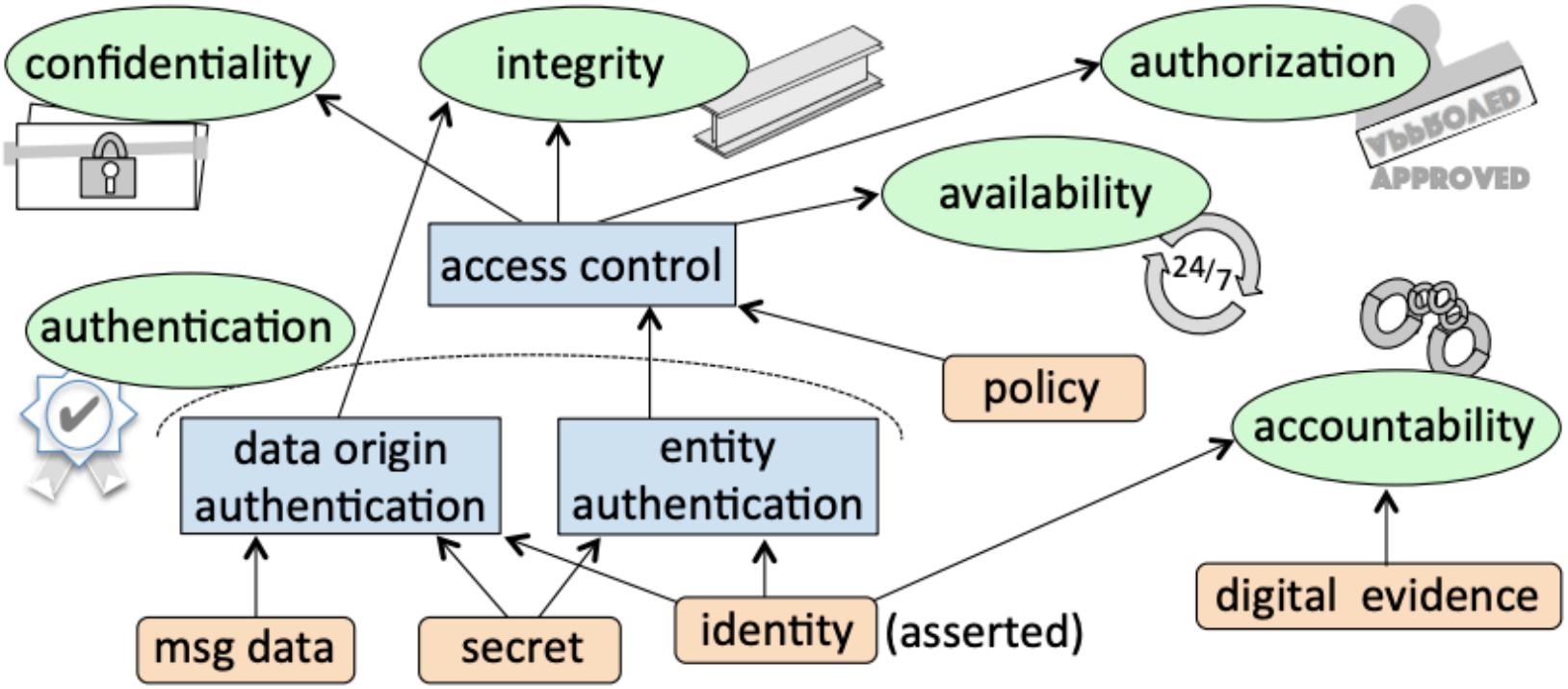
- Disclosure – Unauthorized access to information
- Modification – Unauthorized change of information
- Deception – Acceptance of false data
- Disruption – Interruption or prevention of correct operation
- Usurpation – Unauthorized control of some part of a system

Q. Which type of threats is DDoS?

Security goals

- Confidentiality
  - Property of non-public information remaining accessible only to authorized parties
  - Confidentiality vs. Privacy
    - Privacy narrowly involves personally sensitive information
- Integrity
  - Property of data, software or hardware remaining unaltered, except by authorized parties
- Availability
  - Property of information, services and computing resources remaining accessible for authorized use
- What else?
  - Authorization: property of computing resources being accessible only by authorized entities
  - Authentication: assurance that a principal, data, or software is genuine
  - Accountability; ability to identify principals responsible for past actions

6 high-level security goals



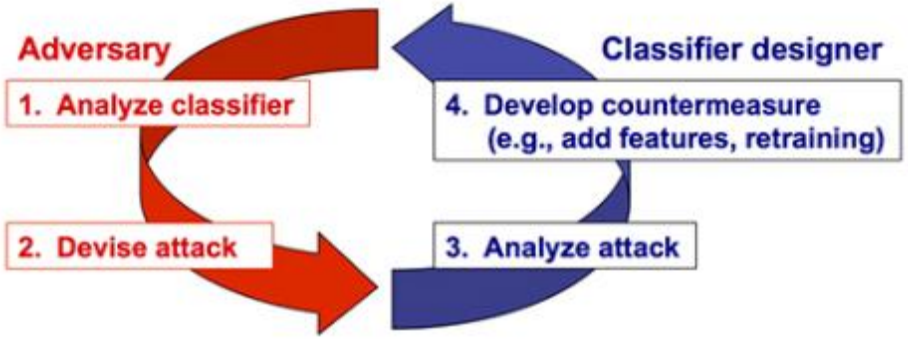
How can we achieve security?

- Prevention: design systems to prevent attacks
  - Cryptography is generally used for this
  - If attack cannot be prevented, increase its cost and control damage
- Detection: detect attackers' violation of security policies
  - Machine learning is generally used for this
- Deterrence (detection + penalty): deter attacks
- Recovery: stop attacks, assess and repair damages

Security is a continuous process

- Arms race between attackers and defenders
- Why?
  - We can achieve security under a certain model (assumption) only
    - New environment might not guarantee the previous model
- No security mechanisms will stop all attacks; attackers just move to new methods and targets
  - Some types of attacks can be eliminated but others will take their place; security mechanisms will fail and new threats will arise
  - The perfect is the enemy of the good (consider mistakes or unforeseen interactions)

An example: learning-based classifiers are not working well



- e.g., analyzing spam detectors → inventing image-based spam against the textual analysis → developing a deep learning-based spam detector

- "Practical Evasion of a Learning-Based Classifier: A Case Study", IEEE S&P (Oakland) 2014
- "Automatically Evading Classifiers: A Case Study on PDF Malware Classifiers", NDSS 2016

Adversary models

- Why do we need adversary models?
  - Attacks and countermeasures are meaningless without
- Elements of an adversary model
  - Security goals (e.g. CIA)
  - Adversary's capabilities
    - computing resources (e.g., CPU, storage, bandwidth)
    - knowledge of keys, passwords, and other secrets (e.g., system/environment design/architecture)
    - opportunity for accessing to the system's components (e.g., source code, run-time behaviours and other implementation details)
    - opportunity for controling to the system's components (e.g., using a service on the target system, modifying messages)

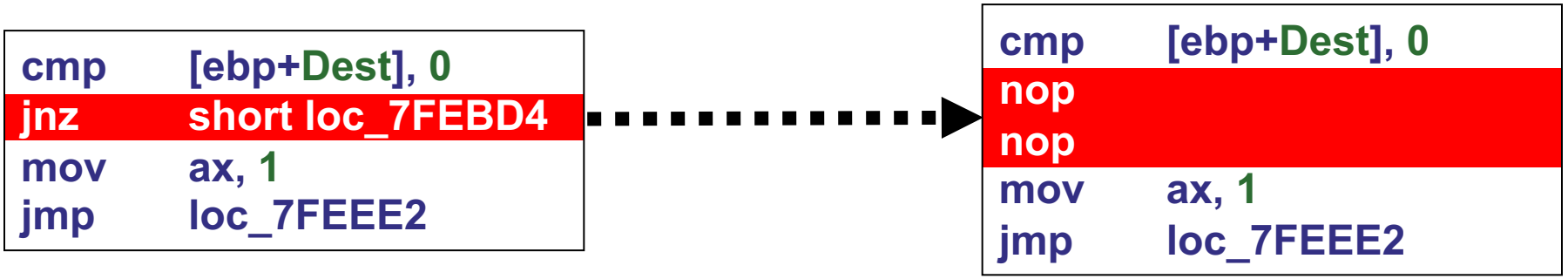
Example: DRM business

- What is DRM (Digital Rights Managements)?
  - Who is the adversary?
- Elements of an adversary model in DRM
  - What are security goals?
    - Authorization (prevention of illegal copy)
  - Adversary's capabilities
    - Knowledge of system and execution environment
    - Access to the protected file and binary code of application
    - Control to some functions of the system (e.g. play)

You are the adversary!

Malicious user can disable DRM protection from the content

We can disable the DRM check logic by replacing the conditional jump with no operations



Original player **Cracked player**

"Bypassing the Integrity Checking of Rights Objects in OMA DRM: a Case Study with the MelOn Music Service", ACM IMCOM 2016

Attack demo

Economic view of adversary models

- Rational attackers compare the cost of an attack with the gains from it
- Rational defenders compare the risk of an attack with the cost of implementing defenses
- But human behavior is not always rational:
  - Don't assume users' perfectly rational behaviors
  - Many cases are explained better by group behavior than rational choice

Example - my office

Security approaches for the office

- Prevention
  - Use a lock to prevent theft
- Detection / Deterrence
  - Identify fingerprints
  - Use CCTV
- Recovery
  - Create redundancy (for important documents)
  - Buy insurance

Perhaps that’s our reality

Questions?


Sungkyunkwan
Campus
Social
Graduate
Professors
English
Confucian
campus
Zone
Sciences
University
Global
Education
Seoul
Natural
Suwon
Korean
School
university
established
edit
also
Humanities
Science
schools
Administration
ASLE-Korea
Academic
Advanced
constructed
Building
Engineering
located
Joseon
Anniversary
Institute
now
two
Hall
Course
lecturers