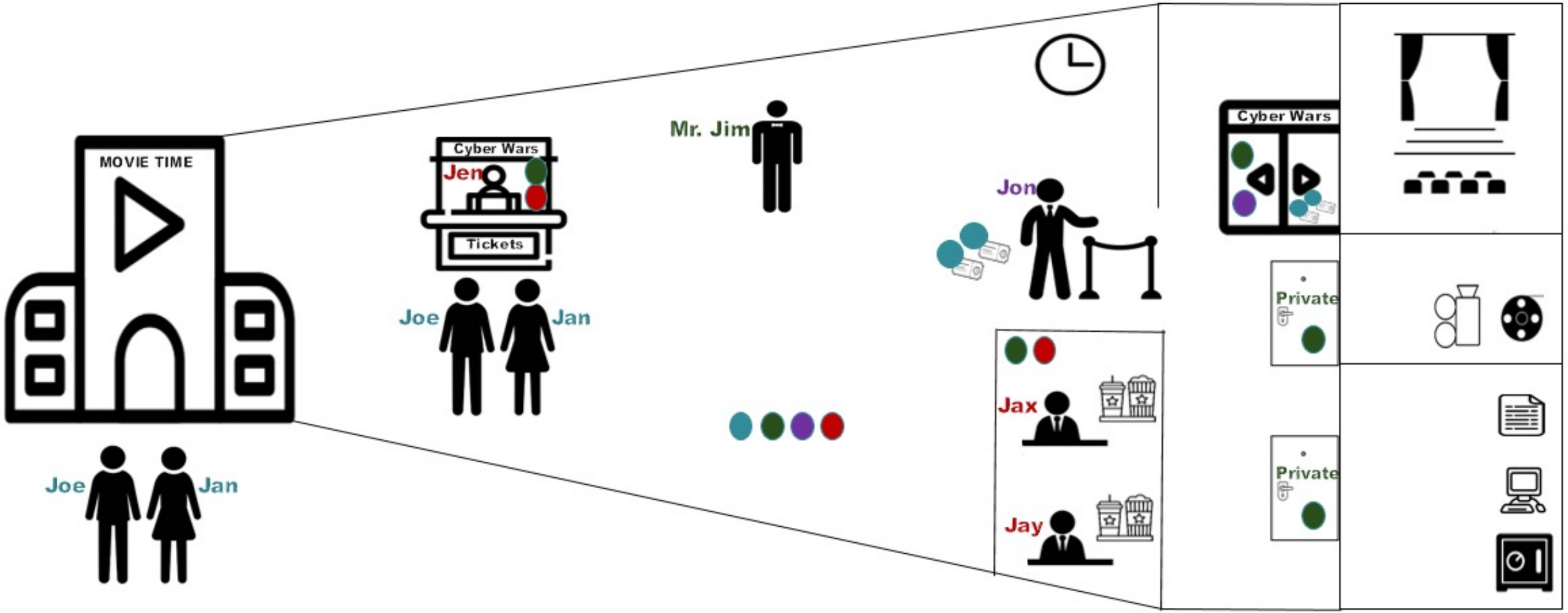
# § 1: Access Control

DANIEL SHIN, ESQ.
CYBERSECURITY RESEARCHER
CENTER FOR LEGAL & COURT TECHNOLOGY


# Prevalence and Importance of Access Control

# Access Control generally






# *The Movie Theater*

# *The Three "A"s of Identity and Access Management*

*Major components of Access Control*

- **Authentication**: the process of determining whether an individual is the person that they say they are.
- **Authorization**: the process of determining access to resources based on the individual's role or credentials within the organization.
- **Accounting**: process of reviewing activities within the organization, especially in areas managed by an Access Control system. Some examples:

# *Different forms of Access Control*

- **Physical Access Controls**: Barriers placed to prevent direct contact with systems.
- **Logical Access Controls**: Hardware and software solutions used to manage access to resources and systems
- **Mandatory Access Controls**: Restricting actions that a subject can perform on an object

# *Different forms of Access Control*

- **Discretionary Access Control**: The owner of a device can determine who can have access control to that device.
- **Role-Based Access Control**: The individual's role (job function) determines his or her access control over organization's resources.
- **Rule-Based Access Control**: A corpus of rules determining individuals' access control over resources.

# Cyber Hygiene Check I

# Cyber Hygiene Check I

John is a database technician. His data center is ringed with a 10-foot-high fence topped with barbed wire. His facility is guarded by security and John is required to show an identification badge to enter the area to park. Once in the building, John must engage in an iris and fingerprint verification scan to open the buildings' automated doors. A second set of automated doors, to prevent tailgating, await John. Once inside his workplace John continues to be surveilled. All doors within the building are locked and swipe card access is required for entry, including his personal office.

Identify all the Access Controls within John's data center.

# Access Control takeaways in Cybersecurity context

# *Principle of Least Privilege*

An individual requesting access to resources should be assigned only the minimum necessary rights to allow that individual to perform their tasks, and for the shortest duration necessary.

# *Principle of Least Privilege*

- Granting permissions to a user beyond the scope of what is necessary can allow that user to obtain or change information in unwanted and unanticipated ways.
- Applying the Principle of Least Privilege within a computer system can mitigate harm from cyber threats.

# *"Need to Know" (Compartmentalization)*

Access is not to be granted unless the individual has a specific need to access the resources to perform a task.

# *"Need to Know"*

- Even if an individual possesses all the necessary approval to access resources, access is nevertheless not to be granted unless the individual has a specific need to access the resources to perform a task.
- "Need to Know" is suitable for highly sensitive information.
  - Classified Information Security's Act.
  - Greatly prevent insider's threat.

# Cyber Hygiene Check II

# Cyber Hygiene Check II

Kim is a legal intern within the legal department of a multinational corporation focusing on cloud computing services. To meet an upcoming deadline, Kim needs to work over the weekend on several privacy documents. With permission, Kim saves the privacy documents on her personal USB flash drive.

Back in the office, Kim accesses the USB flash drive to download the completed privacy documents. To her surprise, a self-executing ransomware begins encrypting all of her files. Kim quickly realizes that her personal storage device was somehow infected and that her privacy documents have been compromised.

# Cyber Hygiene Check II

Which of the following implementation of principles would be most effective in containing the damage caused by the ransomware?

- (A) “Need to Know” (Compartmentalization)
- (B) Principle of Least Privilege
- (C) Physical Access Controls
- (D) Accounting

# Cyber Hygiene Check II

- (A) “Need to Know” (Compartmentalization) – Wrong Answer
- (B) Principle of Least Privilege – Best Answer. By limiting access privileges for Kim, the ransomware can only access and encrypt limited number of files that Kim had write (right to make changes) privileges on. Because Kim did not have write privileges for systems belonging to other departments, the ransomware only damaged a part of the system belonging to the Office of Legal Counsel.
- (C) Physical Access Controls – Wrong Answer
- (D) Accounting – Second Best Answer. If the company’s information security team was monitoring all the activities within the system, the team would detect the unusual encryption activity from Kim’s account and freeze her access privileges, limiting the ransomware’s ability to continue encrypting files.

# Thank you

DANIEL SHIN, ESQ.
CYBERSECURITY RESEARCHER
CENTER FOR LEGAL & COURT TECHNOLOGY