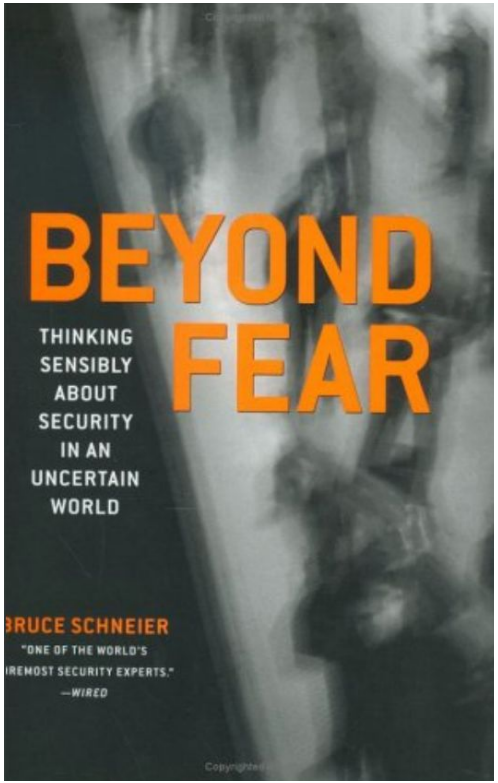
Systems Security I

Beyond Fear



Security and Safety

- Safety is about
  - Assets (things you want to protect)
  - Threats (things that could damage your assets)
- Security is like safety, except that it deals with *intelligent, motivated* threats (“attackers”)
- **This is what makes security hard**

Failure

- Safety and security try to mitigate failure
- They fail when the threat defeats the countermeasure
- Want to make failure hard to induce
  - First two months of the course
- But…
  - No security is perfect
  - Failure will *always* happen

Failure

- But…
  - No security is perfect
  - Failure will *always* happen
- Want systems that *fail well*
- “Failure proof” means “fails badly”
  - Designers didn’t consider failure - assumed it couldn’t happen!
  - Example: Iroquois Theater

Failure

- Examples from the course?

Failure

- Examples from the course
  - Password security - assume database will be stolen
  - ASLR, canaries, etc - assume memory corruption will happen

Showtime!

https://www.youtube.com/watch?v=pIVEUEnIZjM

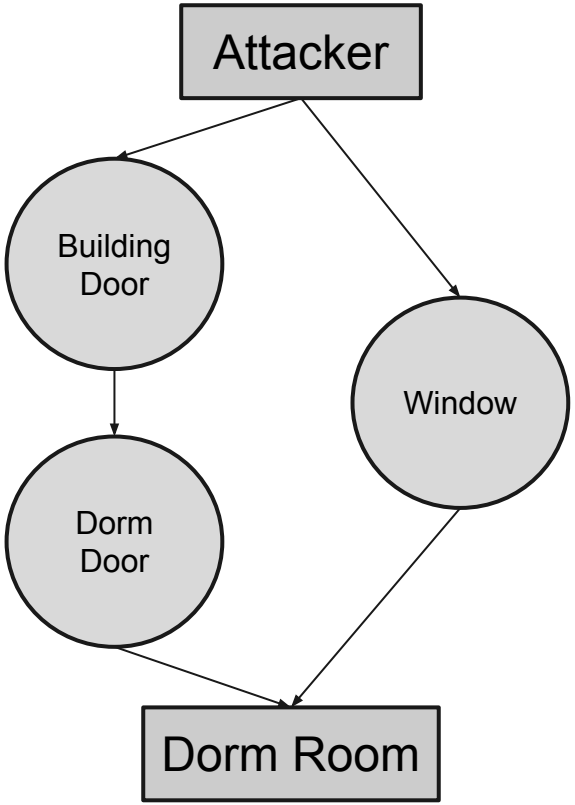
Ocean’s Eleven

- Get inside casino cages
- Through set of doors
  - Each with a 6-digit code changed every 12 hours
- Elevator
  - Fingerprint ID
  - Vocal confirmation from security system and vault
  - Motion detectors in elevator shaft
- Armed guards
- Vault door

Graph Model of Security

- Model security system as graph
- Nodes are security components
- Edges represent reachability
  - After breaking component A
  - You can attack component B

Graph Model of Security



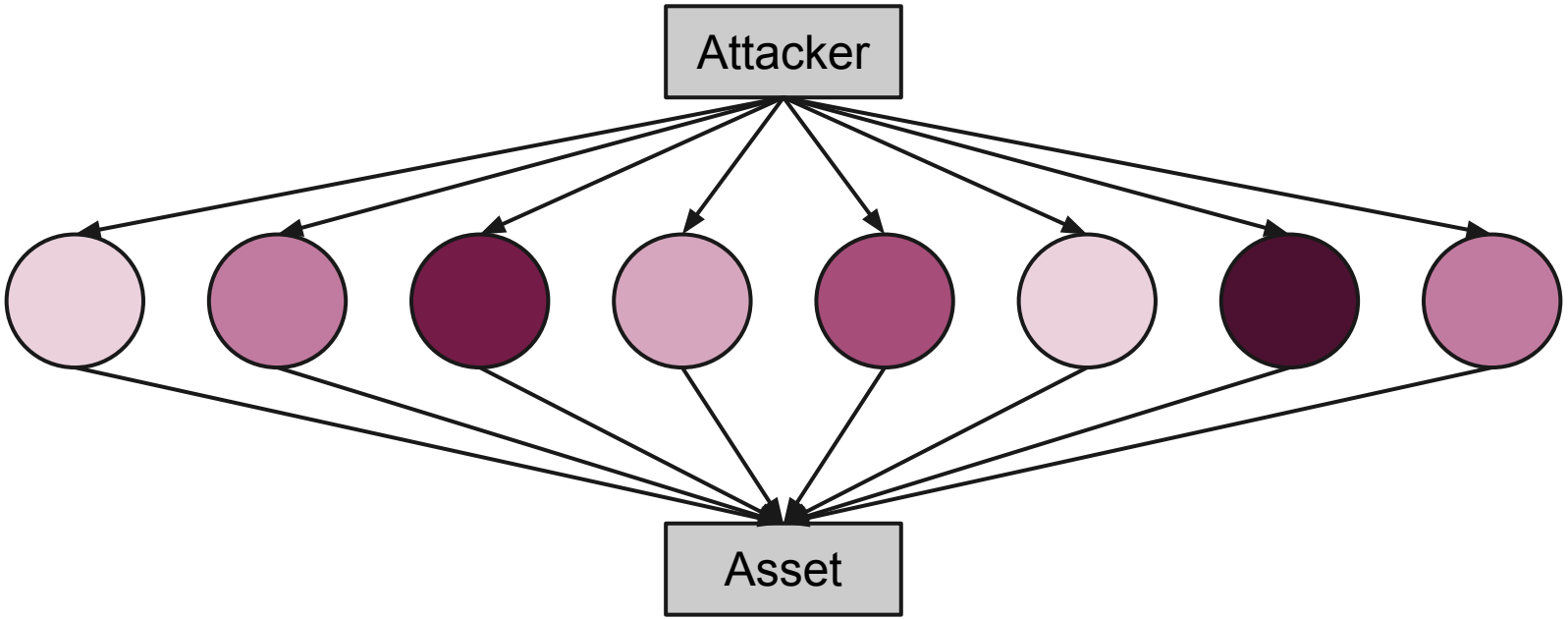
Attack Surface

- Collection of security components immediately accessible to an attacker
- Examples?

Attack Surface

- Collection of security components immediately accessible to an attacker
- Examples
  - Exterior doors, walls, windows of a building
  - Border of a country
  - Computers with publicly-routable IPs

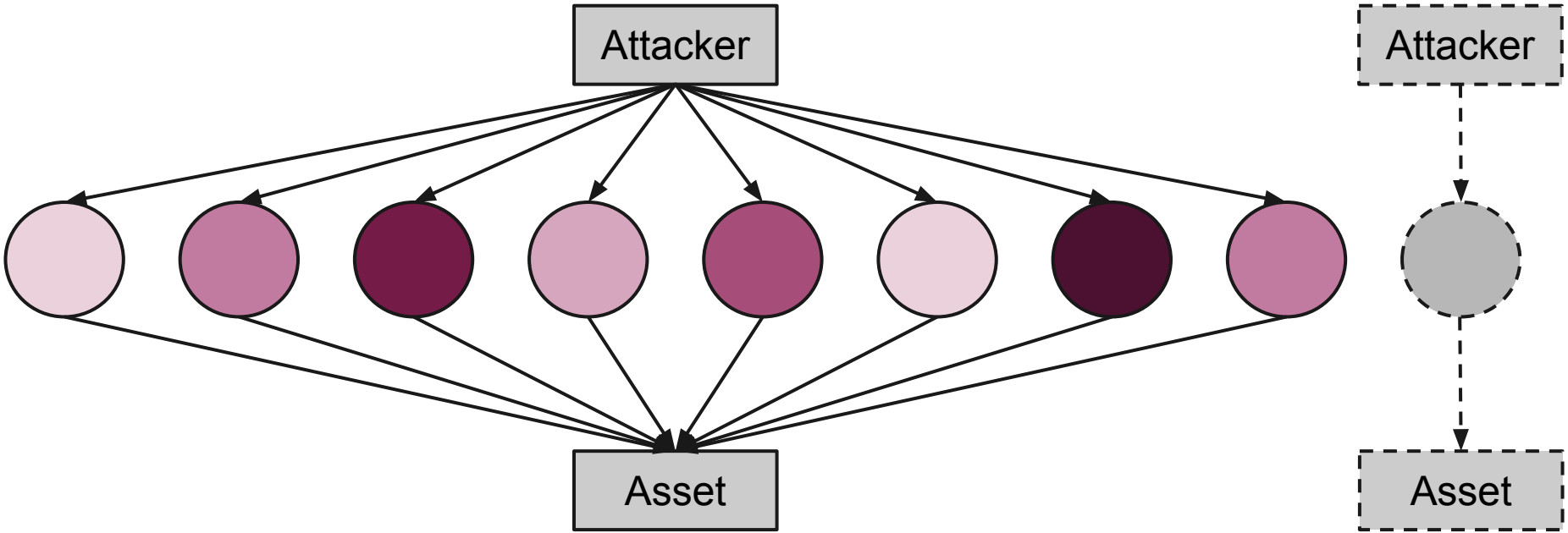
Attack Surface



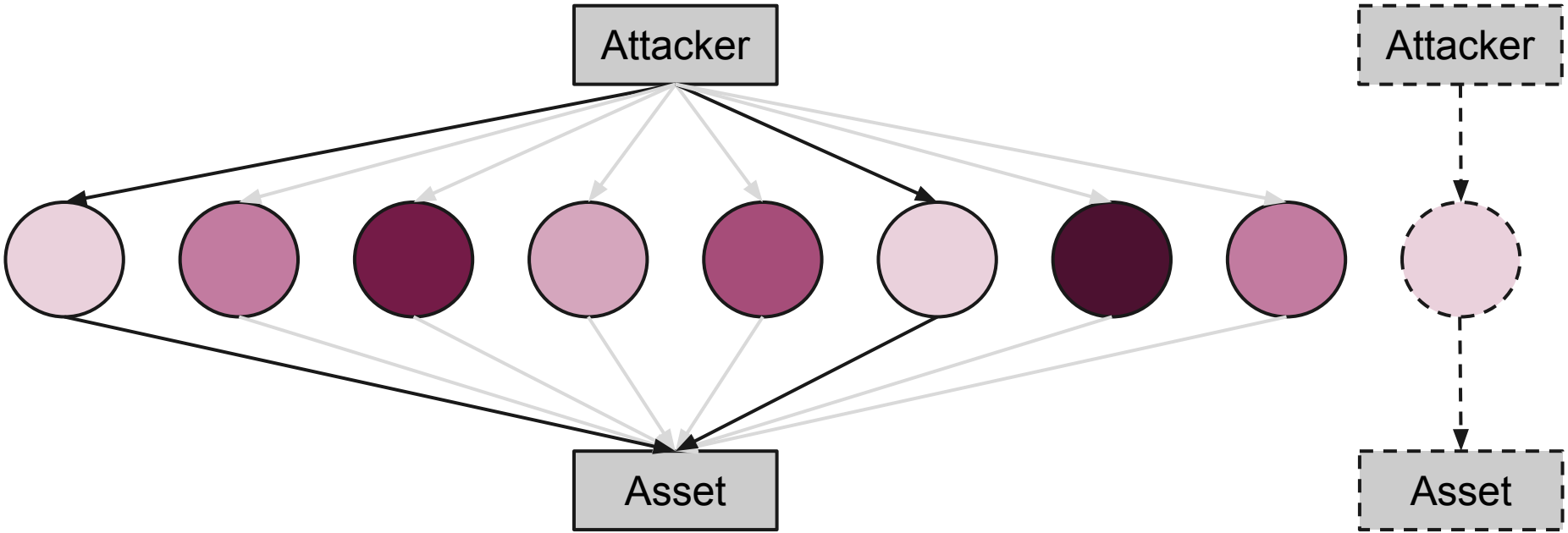
Attack Surface: Weakest Link

- Recall: intelligent, motivated attackers will look for least secure component
- Security is the **minimum** of the components
- “Weakest link in the chain”

Attack Surface: Weakest Link



Attack Surface: Weakest Link



Attack Surface: Weakest Link

- Weakest link in the chain
- Red Example
- Examples?

Attack Surface: Weakest Link

- Weakest link in the chain
- Red Example
- Examples
  - Presidential assassinations
  - Humans in computer security (social engineering)

Attack Surface: Weakest Link

- How can we deal with this?

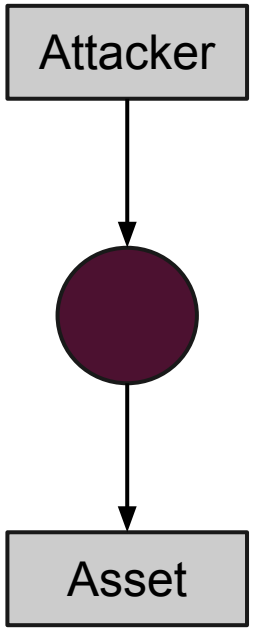
Attack Surface: Weakest Link

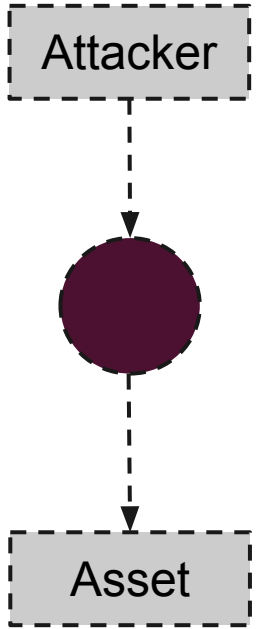
- How can we deal with this?
  - Narrow attack surfaces
  - Eliminate weakest links
  - Choke points

Attack Surface: Narrowness

- Idea:
  - Fewer components
  - Increased security of the expected minimum

Attack Surface: Narrowness





Attack Surface: Narrowness

- Examples?

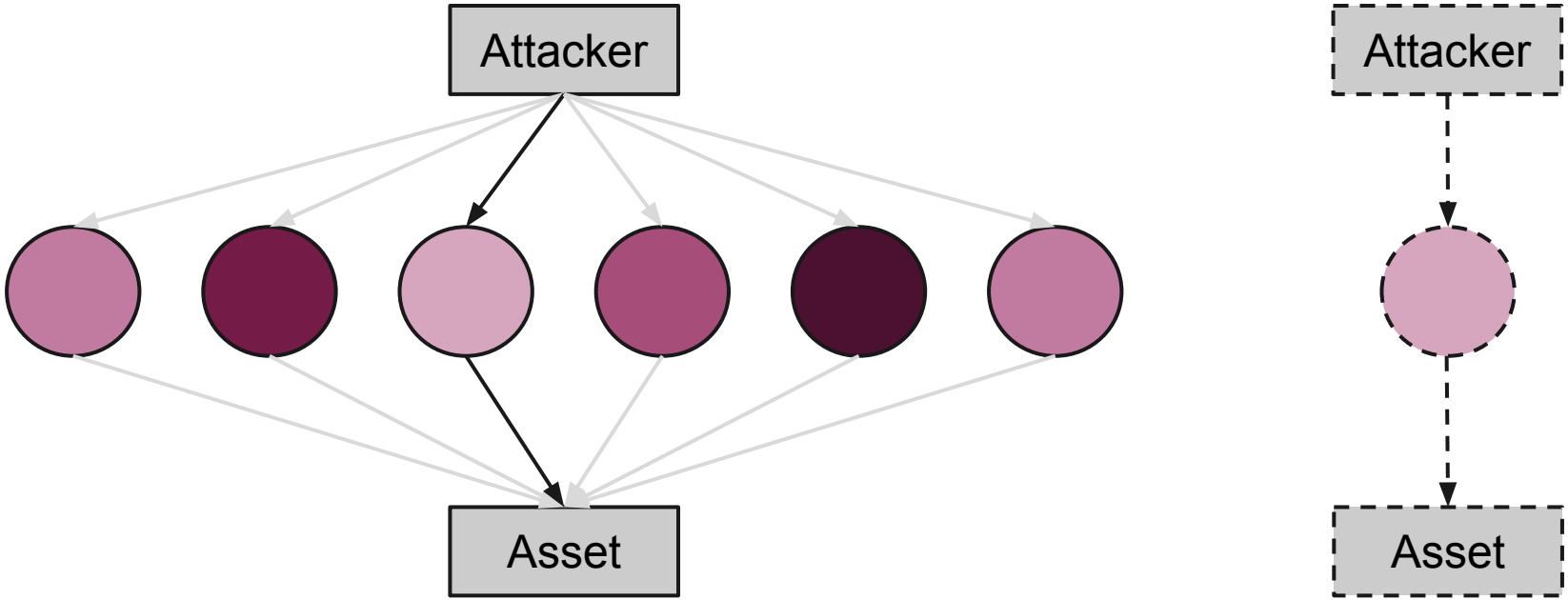
Attack Surface: Narrowness

- Examples
  - Brown Shibboleth (single sign-on)

Attack Surface: Elim. Weakest Links

- Idea: analyze system, remove weakest links

Attack Surface: Elim. Weakest Links



Attack Surface: Elim. Weakest Links

- Examples?

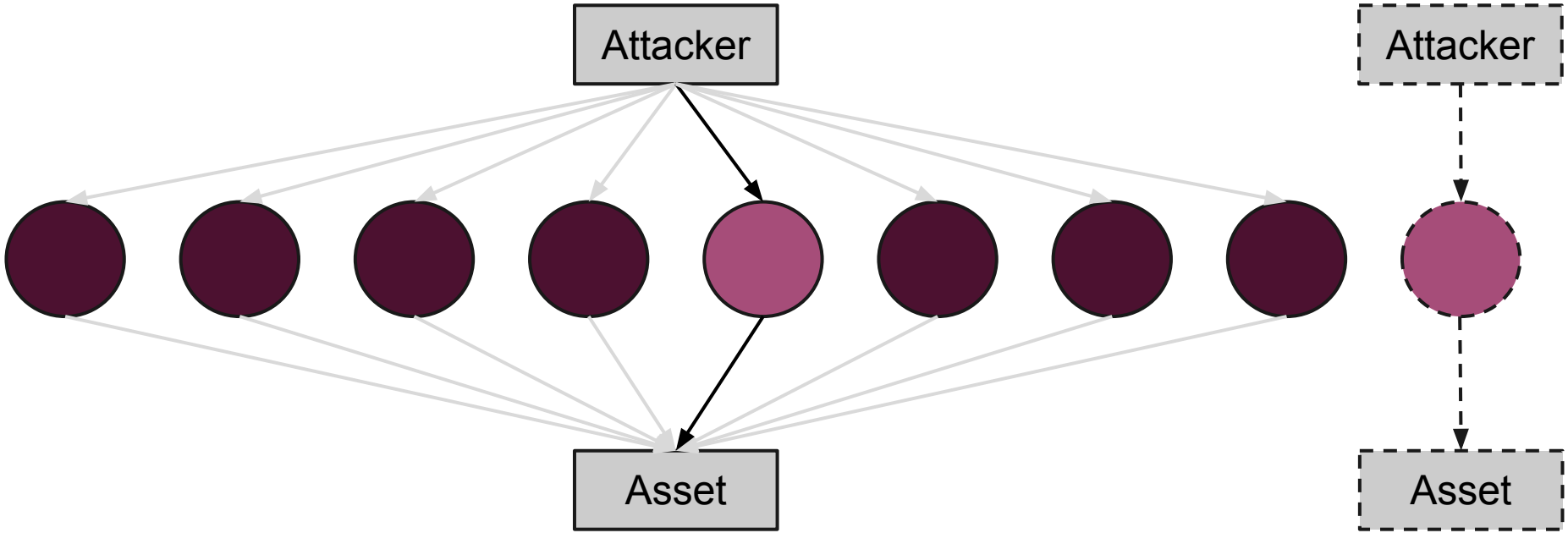
Attack Surface: Elim. Weakest Links

- Examples
  - Removing humans from the loop
  - Chrome removing support for Java/Silverlight plugins

Attack Surface: Choke Points

- Easy to create barriers *nobody* can get past
  - Want to keep your stuff safe? Toss it into the sun!
- Harder to let *only* the authorized parties in
- Idea: make *most* of the attack surface completely impenetrable
- Focus on securing a few access points

Attack Surface: Choke Points



Attack Surface: Choke Points

- Examples?

Chokepoints: Ocean's Eleven

- Get inside casino cages
- Through set of doors
  - Each with a 6-digit code changed every 12 hours
- Elevator
  - Fingerprint ID
  - Vocal confirmation from security system and vault
  - Motion detectors in elevator shaft
- Armed guards
- Vault door

Attack Surface: Choke Points

- Examples
  - Safes/bank vaults
  - Castle walls
  - Border crossings
  - Airport security screening
  - Firewalls
  - Air-gapped networks

Defense in Depth

- Recall: all security will fail
- What happens when it does?
- If the first line of defense is the *only* line of defense, failures will be catastrophic
- Examples?

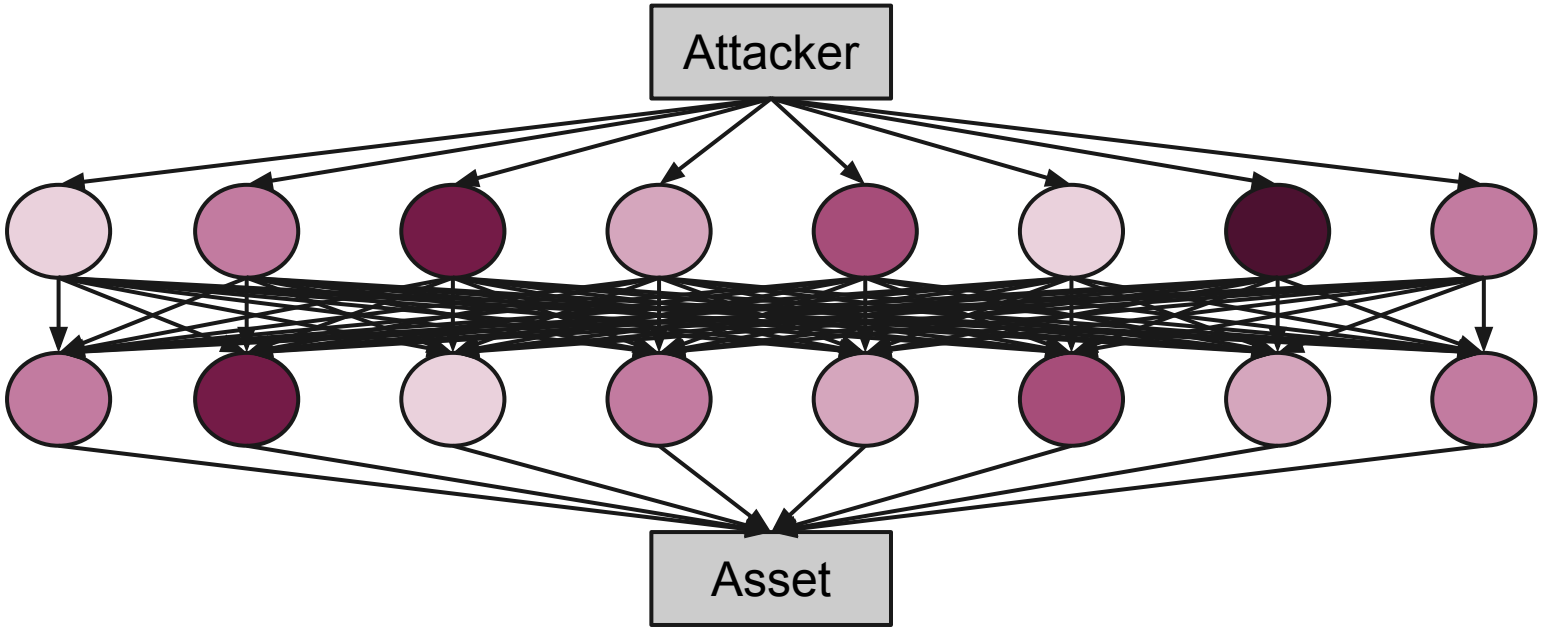
Defense in Depth

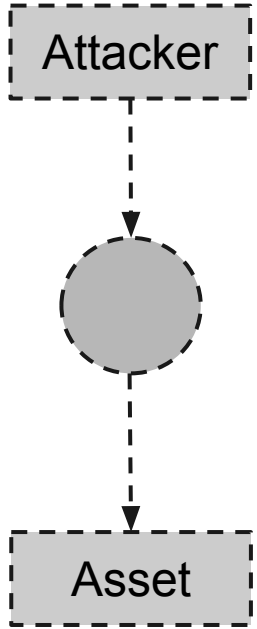
- Recall: all security will fail
- What happens when it does?
- If the first line of defense is the *only* line of defense, failures will be catastrophic
- Examples
  - Maginot line
  - Iroquois Theater
  - VPNs

Defense in Depth

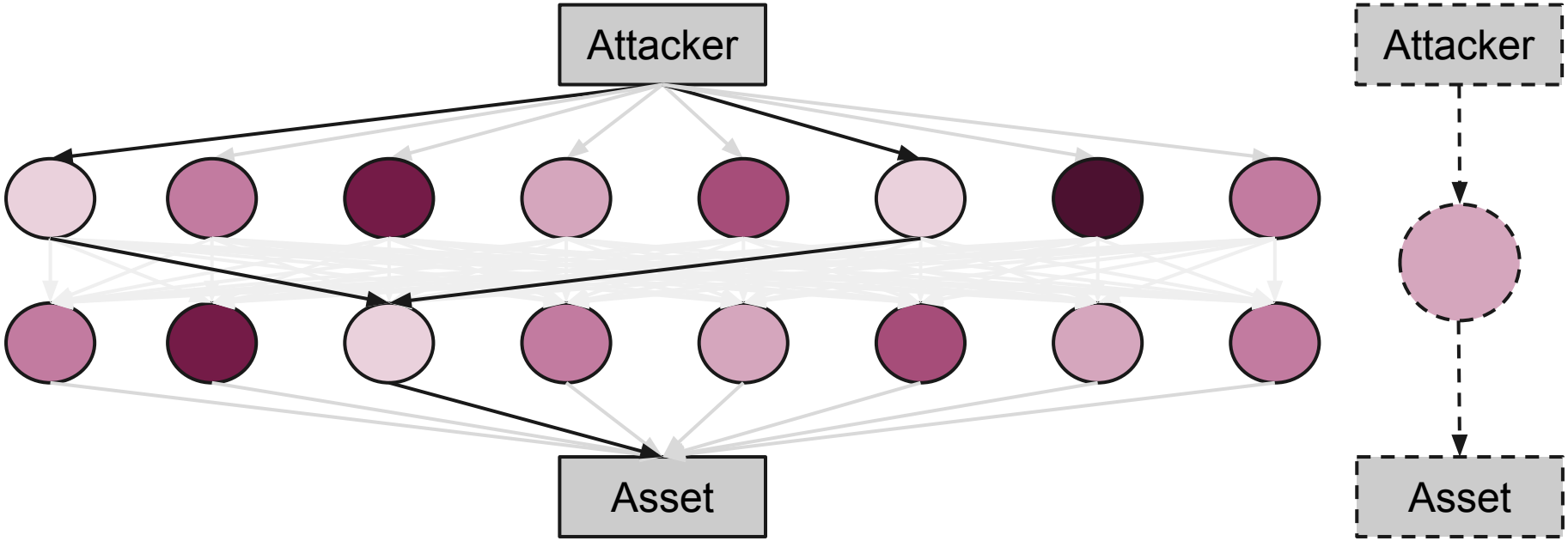
- Instead, layer defenses
- Attackers must defeat all layers
- Security is the **sum** of the layers
  - Security of each layer is still the minimum

Defense in Depth





Defense in Depth



Defense in Depth

- Protecting the Sorcerer's Stone
  - Fluffy the three-headed dog
  - Devil's snare plants
  - Locked door with flying keys
  - Giant chess game
  - Troll
  - Logic problem with potions
  - Magic mirror
- Other examples?

Ocean’s Eleven

- Get inside casino cages
- Through set of doors
  - Each with a 6-digit code changed every 12 hours
- Elevator
  - Fingerprint ID
  - Vocal confirmation from security system and vault
  - Motion detectors in elevator shaft
- Armed guards
- Vault door

Defense in Depth

- Other examples
  - Two-factor authentication
  - Antivirus
  - Memory corruption protections
    - Canaries
    - ASLR
    - etc

Defense in Depth

- Layers should be heterogeneous
- Layers of the same type will have similar vulnerabilities
- Increase the number of skills needed
  - Decrease probability the attacker will have all skills
  - Increase time to attack
- Examples?

Defense in Depth

- Examples
  - Castle wall and moat
  - Securing password databases and hashing

Defense in Depth

- Sometimes, defenses strengthen each other
- Pop quiz: why does TSA limit liquid to 3oz?
- Other examples?

Defense in Depth

- Sometimes, defenses strengthen each other
- Pop quiz: why does TSA limit liquid to 3oz?
- Other examples
  - Safes and guards
  - Passwords and password lockouts