Defense in Depth

If at first you don’t succeed, try, try again

Outline

- Security and Safety
- Failure
- Weakest Link
- Defense in Depth
- Compartmentalization
- Prevention vs Detection

Showtime!

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

Oceans 11

- 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

Security ⊂ Safety

- Safety is about:
  - Assets (things you want to protect)
  - Threats (things that could damage your assets)
- Examples:
  - A building's foundation
    - Protects inside (asset) against rain water (threat)
  - A climbing harness
    - Protects climber (asset) against fall (threat)

Security ⊂ Safety

- Security is the subset of safety that deals with *intelligent*, *motivated* threats (“attackers”)
- **This is what makes security hard**
- Examples:
  - If rain was intelligent, it would fall sideways through the crack under your front door
  - An intelligent attacker would cut the climber’s rope

Failure

- Safety and security try to mitigate failure
- They fail when the threat bypasses the defense
- Want to make failure unlikely/hard to induce
- But failure will *always* happen
- So you want a system that will *fail well*

Failure

- No safety/security is perfect
- Will *always* fail under the right conditions
- “Failure-proof” usually means “fails badly” because the designers didn’t consider failure (they thought it was impossible)
- Example: Iroquois Theater

Weakest Link

- With safety, only have to protect against probable threats
- Example:
  - Unlikely that a strong wind will blow rain under door
  - Unlikely that a knife will happen to fall and cut climber's rope

Weakest Link

- With security, attackers are intelligent
- They may induce things to happen that would be very unlikely by pure chance
- **A rational attacker will seek out the easiest or most likely to succeed attack**
- The defense which is easiest to defeat is called the *weakest link*

Weakest Link

- Just like in a real chain, a security system is only as strong as its weakest link
- Examples?

Weakest Link

- Just like in a real chain, a security system is only as strong as its weakest link
- Example:
  - Protecting the president from assassination is hard.
  - It's very easy to protect the Oval Office
  - It's hard to protect them during a public speech
  - Making the Oval Office more secure won't help
  - Assassinations often succeed, usually in public

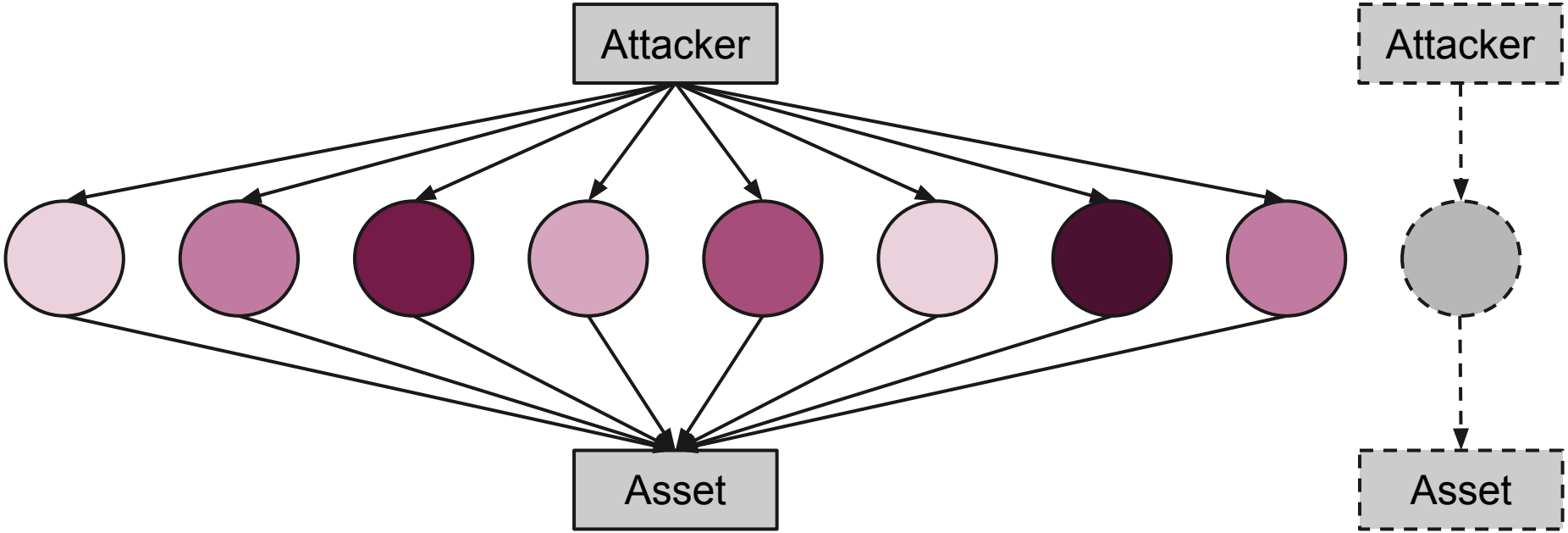
Weakest Link 11

- 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

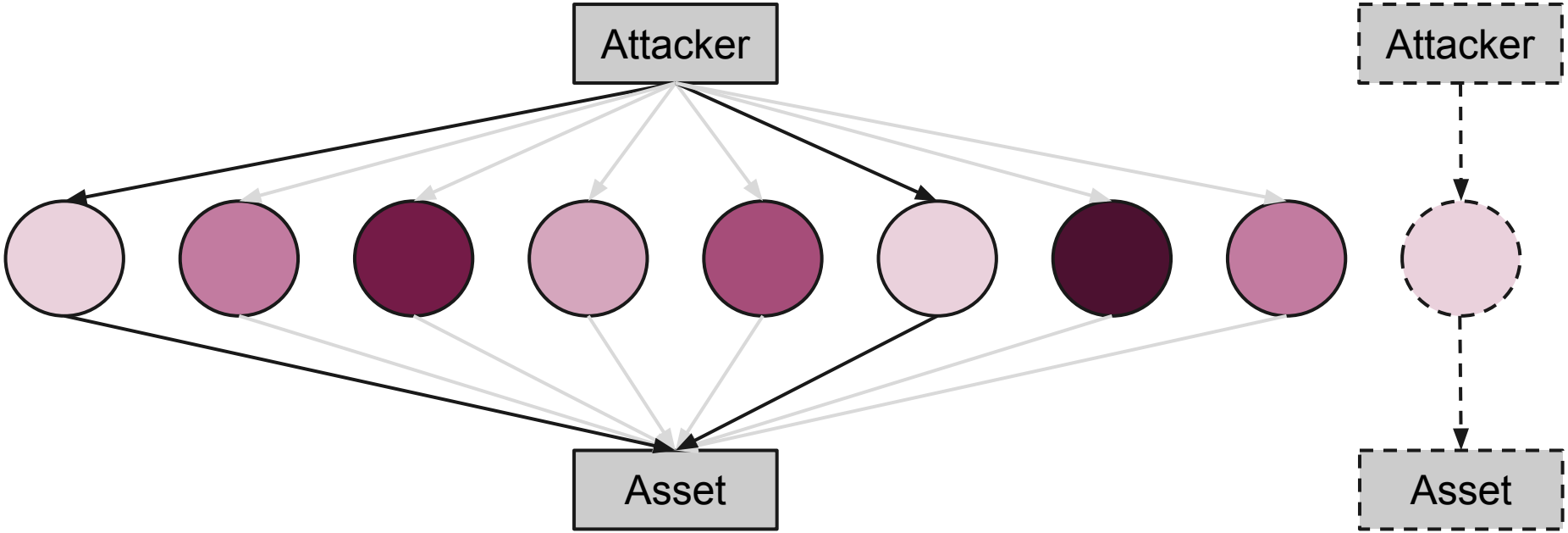
Weakest Link

- *Attack surface* - collection of places an attacker could attack
- Attack surfaces can be *wide* or *narrow*
- Security is the **minimum** of the components

Weakest Link



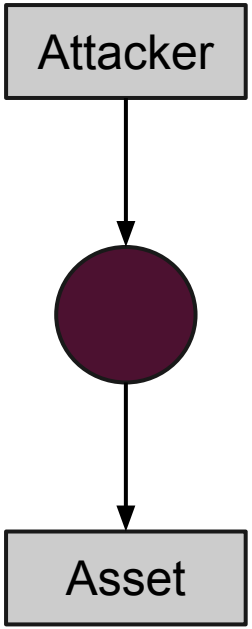
Weakest Link

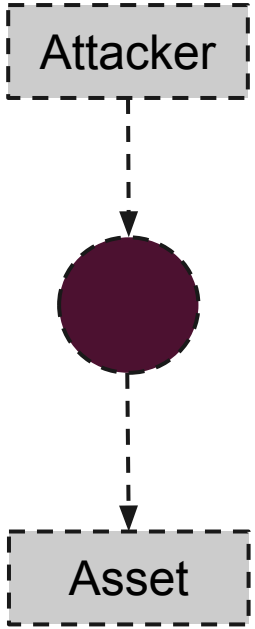


Weakest Link

- Design systems with small attack surfaces
- Example: Brown Shibboleth single sign-on
  - Each service (Workday, The Critical Review, etc) could implement its own sign on, but then *each* would be part of the attack surface
  - Instead, in order to access any of those, you have to go through Shibboleth

Weakest Link

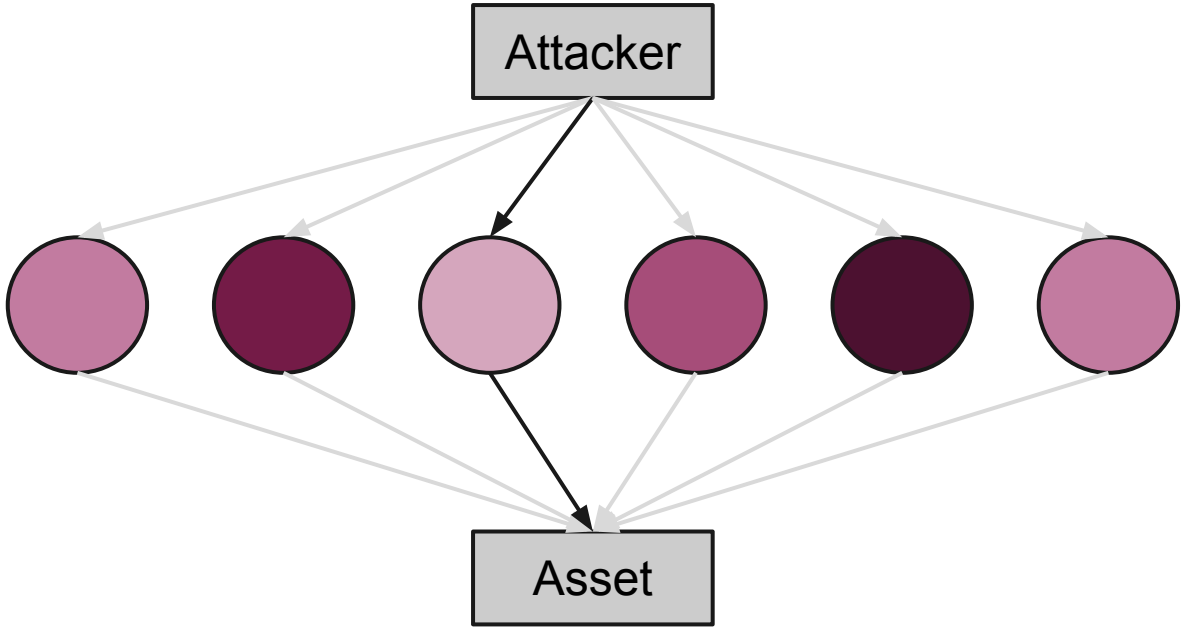


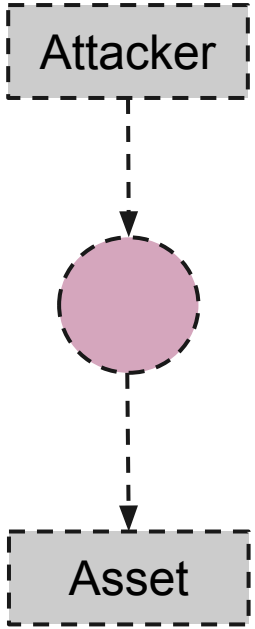


Weakest Link

- If you can’t design a small attack surface, work to strengthen or eliminate weakest links

Weakest Link

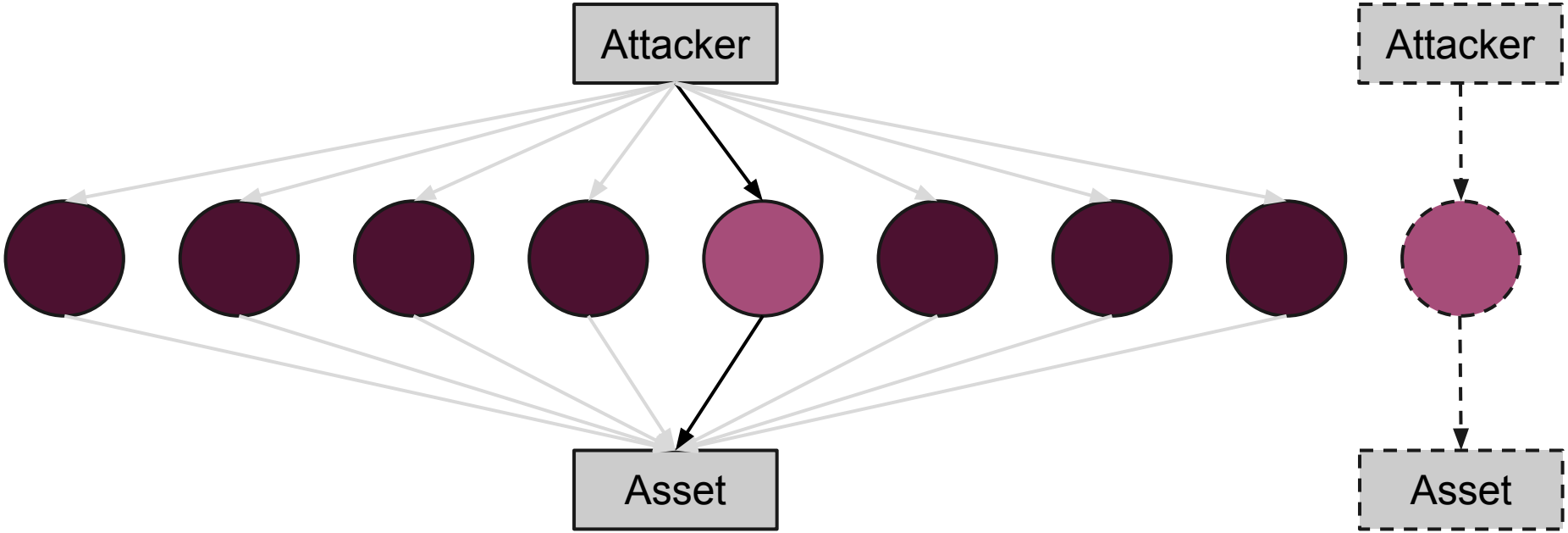




Weakest Link

- Create *choke points*
- Very easy to create impenetrable barriers that *nobody* can get through
- Not very useful - you want the right people to get through
- Use these impenetrable barriers everywhere except for a few places

Weakest Link



Weakest Link

- Examples?

Weakest Link

- Example
  - Firewalls limit network access to only certain ports
  - Other ports are blocked to *everybody* - even authorized users
  - Limits attack surface to open ports

Weakest Link 11

- 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

- Must assume security will fail
- If you rely solely on one defense, its failure will be catastrophic
- Examples?

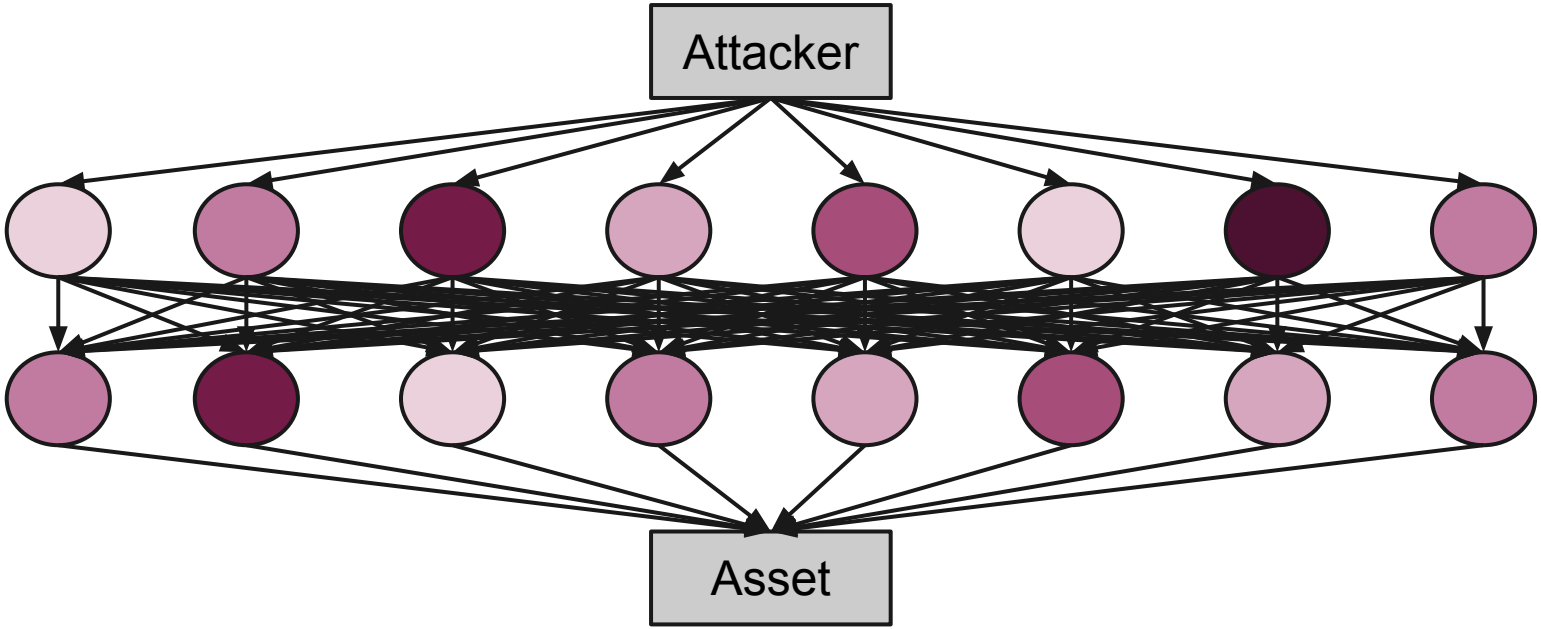
Defense in Depth

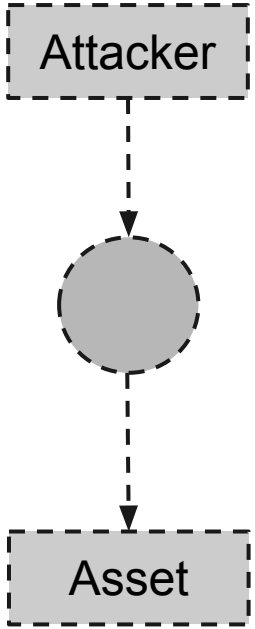
- Must assume security will fail
- If you rely solely on one defense, its failure will be catastrophic
- Example: Maginot Line

Defense in Depth

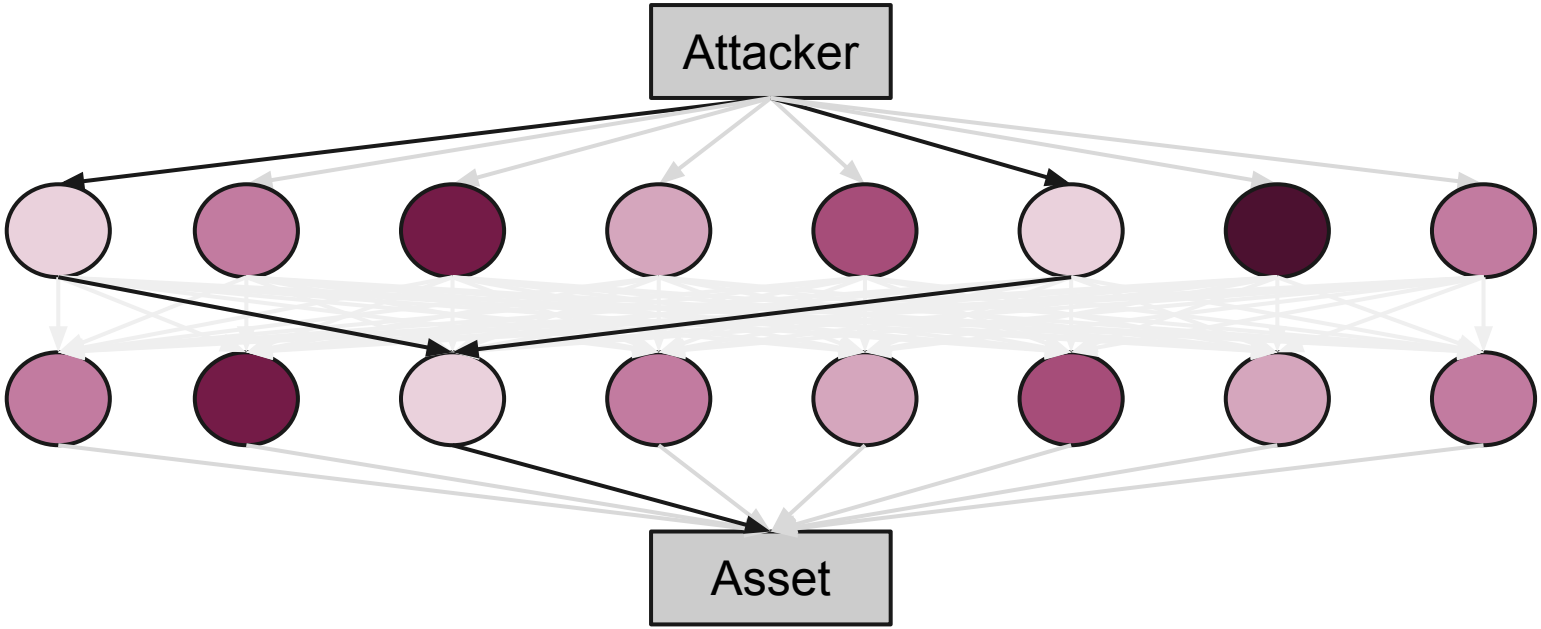
- Instead, *layer* your defenses
- If one defense fails, another is still in the attacker's way
- Security is the **sum** of the layers
  - But each layer is still the minimum of its components (weakest link)

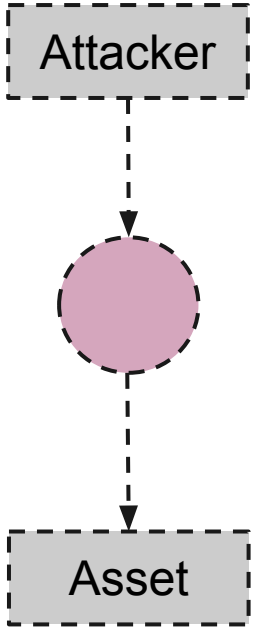
Defense in Depth





Defense in Depth





Defense in Depth

- Examples?

Defense in Depth

- Examples:
  - Two-factor authentication
  - Best practice for servers: ssh key to log in, password to get root

Defense in Depth

- Layers should be heterogeneous
- Multiple layers of the same type are usually weaker - attacker can reuse attack
- Increase the number of skills needed
- Reduce the probability that an attacker has all of those skills

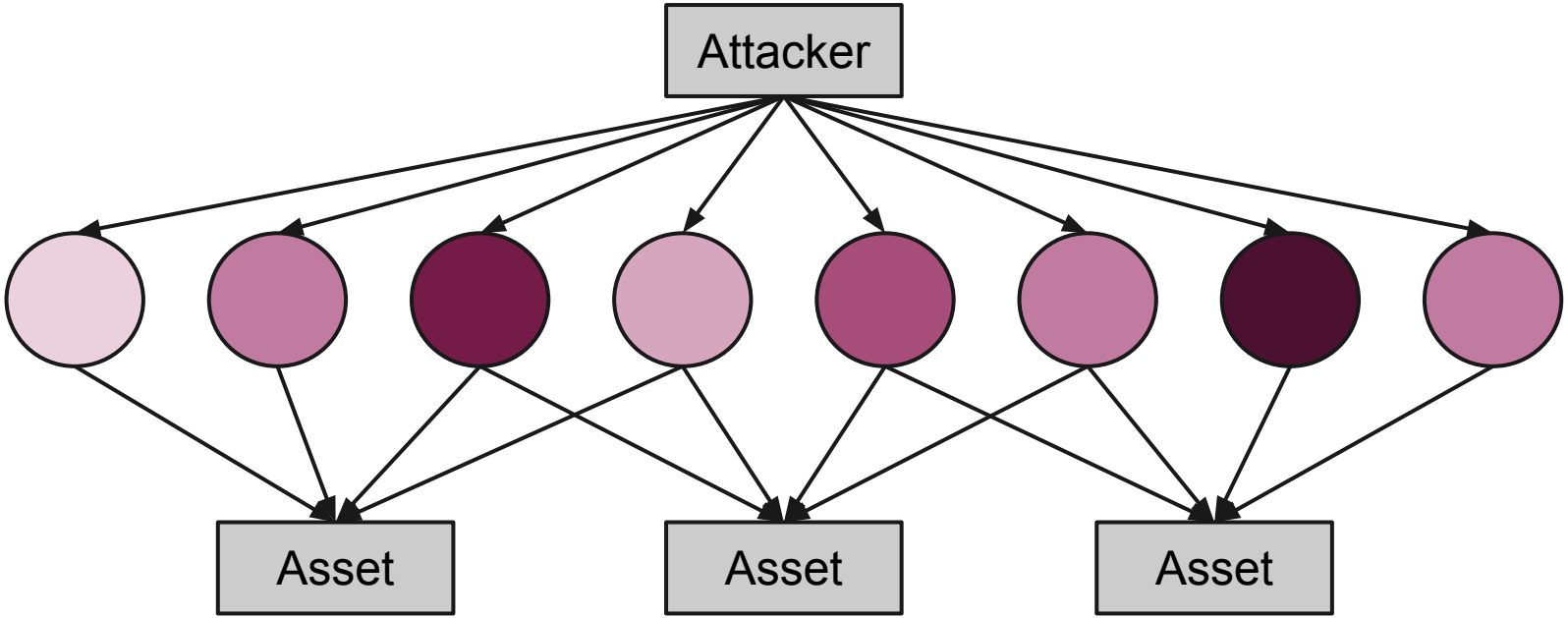
Defense in Depth 11

- 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

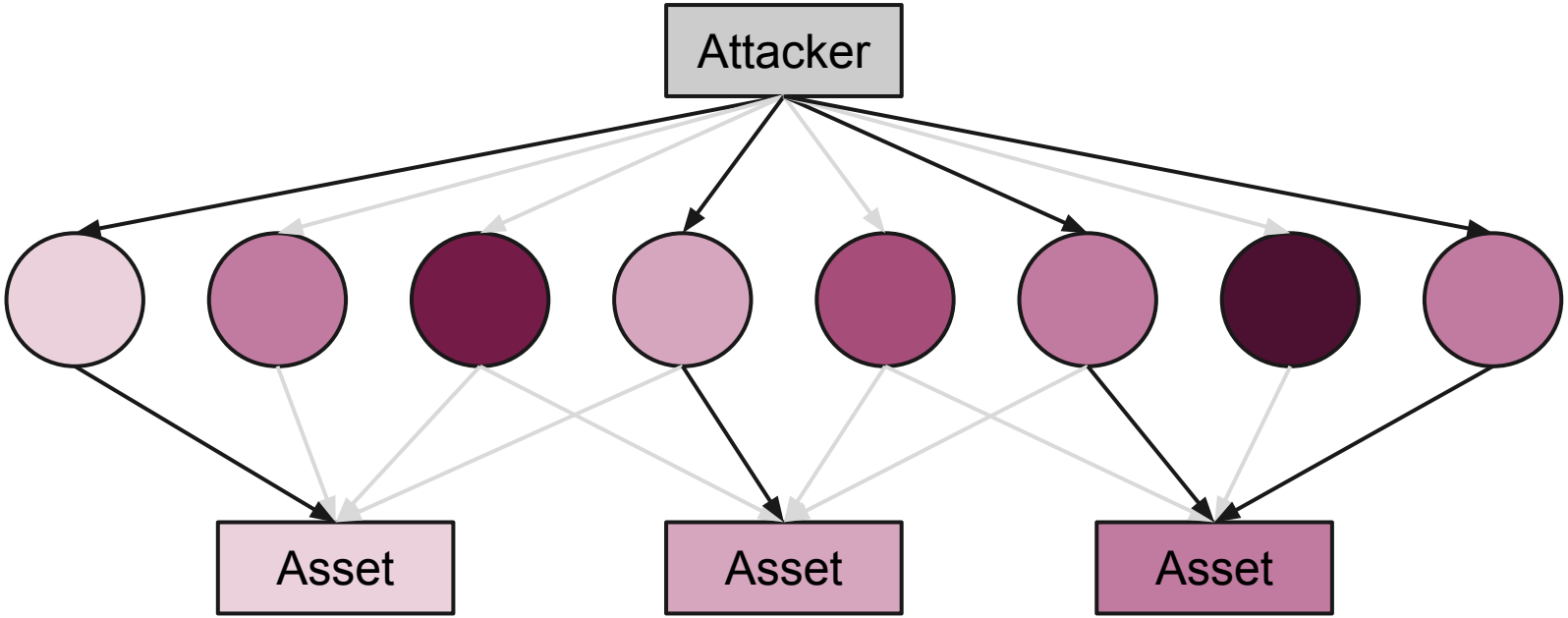
Compartmentalization

- A special form of defense in depth
- Secure assets separately
- Have to attack them independently
- Limit damage from an attack

Compartmentalization



Compartmentalization



Compartmentalization

- Examples?

Compartmentalization

- Examples:
  - Travelers often split money - some in wallet, some in backpack, etc
  - Street drug dealers handle drugs and money separately
  - Top-secret information is given out on clearance plus “need to know”
  - Each office has a different key

Compartmentalization 11

- 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

Prevention vs Detection

- Some defenses are *preventative* - aim to stop attackers from getting inside a system
- Generally passive - work just by existing
- Examples?

Prevention vs Detection

- Some defenses are *preventative* - aim to stop attackers from getting inside a system
- Generally passive - work just by existing
- Examples:
  - Walls
  - Doors
  - Firewalls

Prevention vs Detection

- Others *detect* threats, and respond
- Examples?

Prevention vs Detection

- Others *detect* threats, and respond
- Examples:
  - Security guards
  - Antivirus software

Prevention vs Detection

- Prevention is *really hard* to do perfectly
- Consider protecting the president - even though a ton of effort is put in by very skilled organizations, it often fails
- Prevention is best coupled with detection

Prevention vs Detection

- Prevention is best coupled with detection
- Safes are rated based on time
  - “TL 30” - a professional safecracker with tools will take 30 minutes to crack
  - “TL-TR 60” - resist the same safecracker with an oxyacetylene torch for 60 minutes
- Gives enough time for the guards to notice
- No guard? Anyone will crack it *eventually*

Prevention vs Detection

- Detection allows:
  - Response - mitigate the threat (delete the virus)
  - Analysis - know that you were breached and figure out how so you can fix it
  - Punishment - punish attackers to deter future attackers
    - Requires attribution; usually doesn't happen on the internet

Prevention vs Detection

- Examples?

Prevention vs Detection

- Examples:
  - Average APT compromise is ~1 year[1]
  - Deep Packet Inspection (DPI)
  - Password attempt lockouts

1 https://en.wikipedia.org/wiki/Advanced_persistent_threat

Prevention vs Detection 11

“Say we get into the cage, and through the security doors there, and down the elevator we can’t move, and past the guards with the guns, and into the vault we can’t open. Say we do all that. We’re just supposed to walk out of there with $150 million in cash on us without getting stopped?”

Prevention vs Detection

- Detection without prevention is *risky*
- This is especially true in computer security
- As a general rule, computer security is far better at prevention than detection
- Be wary of claims that tech like DPI are a panacea
- Detection to *augment prevention* is great

Review

- Security and Safety
- Failure
- Weakest Link
- Defense in Depth
- Compartmentalization
- Prevention vs Detection

Suggested Reading

Beyond Fear by Bruce Schneier