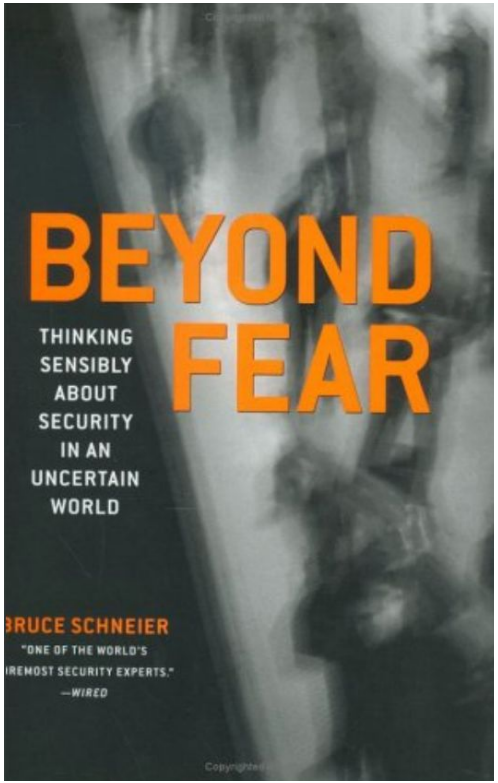
Systems Security II

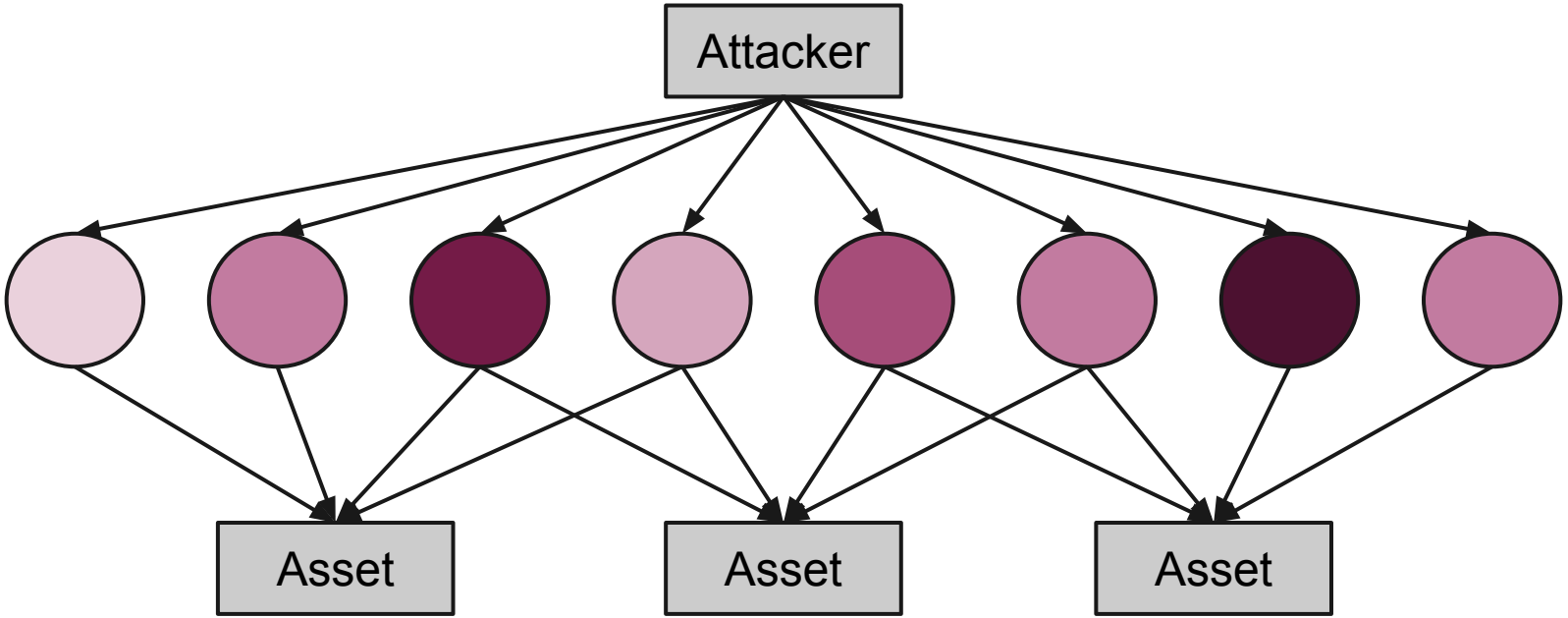
Beyond Fear



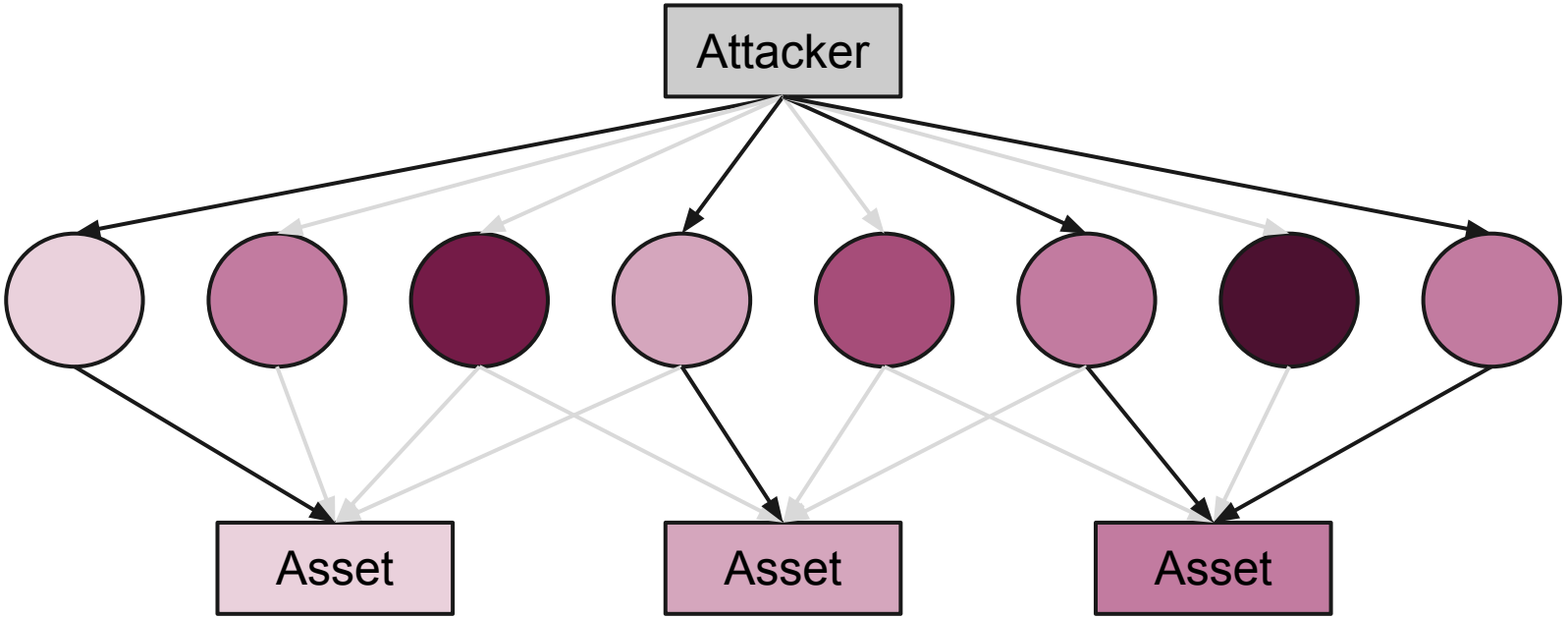
Compartmentalization

- Similar to defense in depth
- Secure various assets separately
- Compromising one asset doesn't necessarily allow an attacker to compromise others

Compartmentalization



Compartmentalization



Compartmentalization

- Non-technical examples?

Compartmentalization

- Non-technical examples
  - Travelers' money
  - Street drug dealers (separating money and drugs)
  - Top-secret information: clearance plus "need to know"
  - Offices with separate keys

Compartmentalization

- Technical examples?

Compartmentalization

- Technical examples
  - Beyond Corp vs VPNs
  - Untrusted software isolation
    - VMs
    - AppArmor

Compartmentalization

- Different assets deserve different security
- Examples?

Compartmentalization

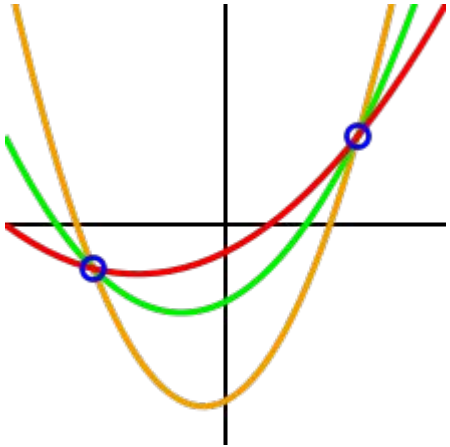
- Different assets deserve different security
- Examples
  - Master keying systems
  - Certificate trees

Secret Sharing

- DNSSEC is a certificate hierarchy for DNS
- Single DNSSEC root
- Root key is split so that 5 of 7 people must convene in order to reconstruct it
- *Secret sharing*

Shamir Secret Sharing

- Key insights:
  - Any *k* distinct points define a *k - 1* degree polynomial
  - Given < *k* points, all *k - 1* degree polynomials are equally likely



https://upload.wikimedia.org/wikipedia/commons/thumb/6/66/3_polynomials_of_degree_2_through_2_points.svg/220px-3_polynomials_of_degree_2_through_2_points.svg.png

Shamir Secret Sharing

- Generate a random *k - 1* degree polynomial
  - The description of this polynomial is the secret key
- Pick *S* random points on the curve
- Each point is a secret
- Any *k* of the *S* points are sufficient to reconstruct the key

Detection and Response

- Who here is murder-proof?
- Whose house/apartment/dorm is burglary-proof?
- How much do you worry about being murdered or burgled?
- Why?

Detection and Response

- Good prevention is *hard* (and expensive)
- “Detection works where prevention fails”
- Often, detection and response are cheaper and more effective

Detection and Response

- Example: 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*
- “Our job is to slow ’em down or make ’em make a lot of noise”

Detection and Response

- Other examples?

Detection and Response

- Response
  - Reaction
  - Mitigation
  - Recovery
  - Forensics
  - Counterattack
- Examples?

Detection and Response

- Response
  - Reaction: security guards
  - Mitigation: increasing security, disabling services
  - Recovery: backups, changing passwords, etc
  - Forensics: find out who did it
  - Counterattack: prosecute them

Detection and Response

- Belgian jewelry thieves

Detection and Response

San Jose, Costa Rica