Illegitimi Non Irritatum

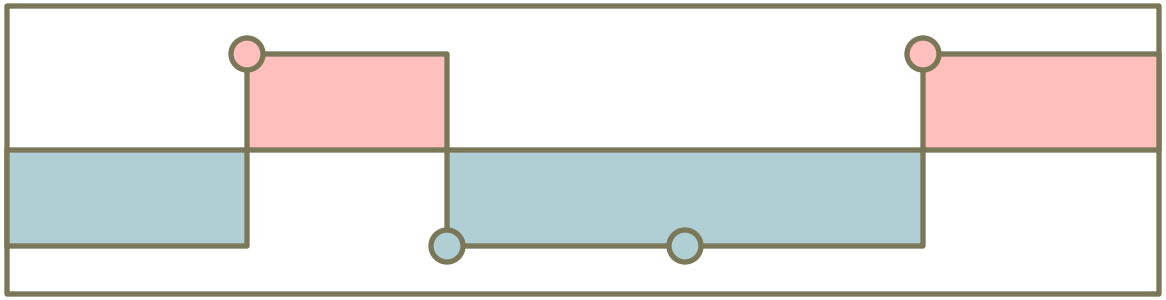
(aut Lorem Ipsum Deserta Omnium)

Orr Dunkelman and Moses Liskov

Cyber security is all the same!

- As cyber defenders, we alternately:
  - Take costly actions to improve our security, and
  - Rely on inaction (or free/cheap actions)
- As cyber attackers, we alternately:
  - Take costly actions to illegitimately obtain resources, or
  - Avoid exposure and take what we can get
- These are really the same thing!

FlipIt: a security game [JORvD]

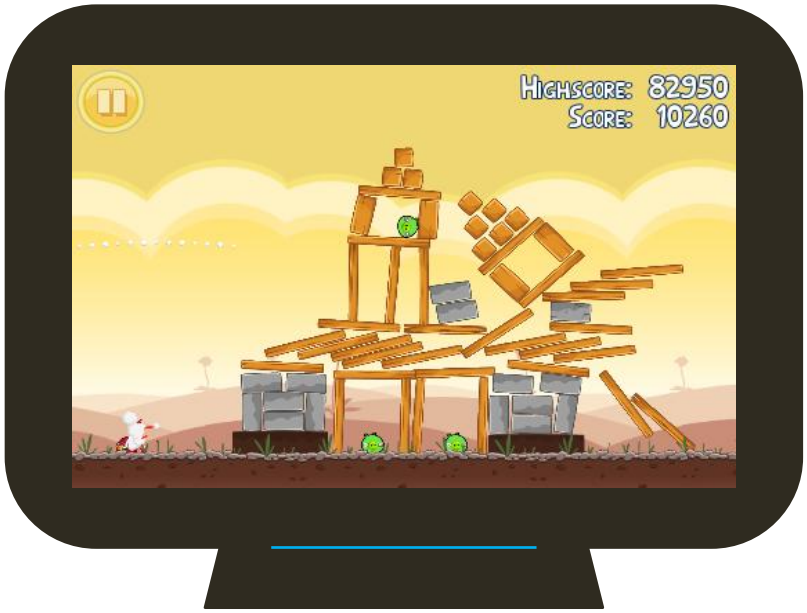


- Players make moves to obtain the resource
- Players are unaware of their opponents' moves until they move
- Attacker and defender have costs c_0 and c_1 for making moves
- Goal: maximize benefit (period of control – costs)
- Interesting results about optimal strategies [JORvD]…

Coöperati Humanes Est

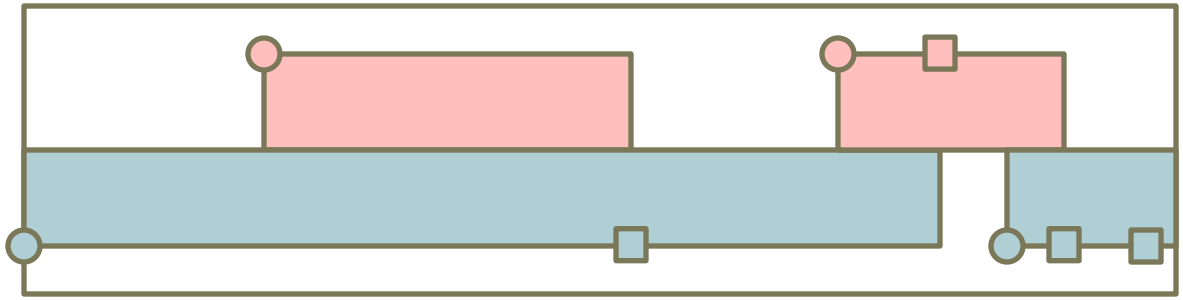
(to share is human)

- In `FlipIt`, only difference between attacker and defender are differing costs.



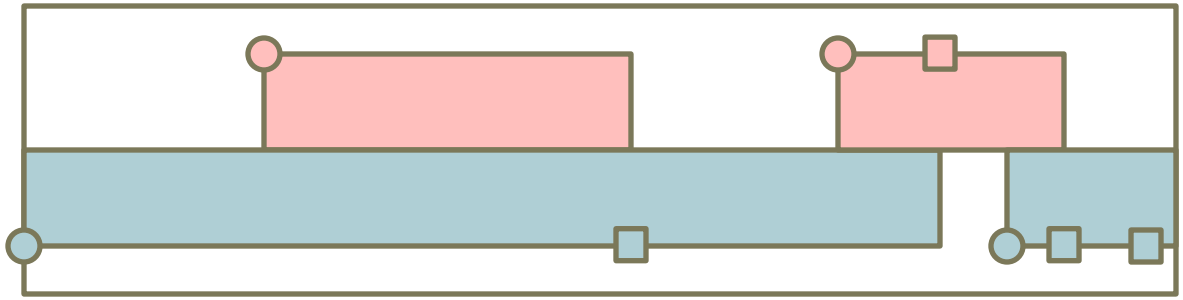
- Both attacker and defender can benefit!
- … unless the move isn't stealthy.

A new game



- Player i can make two moves:
  - Obtain access (for cost a_i)
  - If we have access: lock down (for cost b_i)
- Players know when they lose access
- Players learn that their opponent has access only when they lock down
- Players benefit for having access
- Goal: Maximize benefit

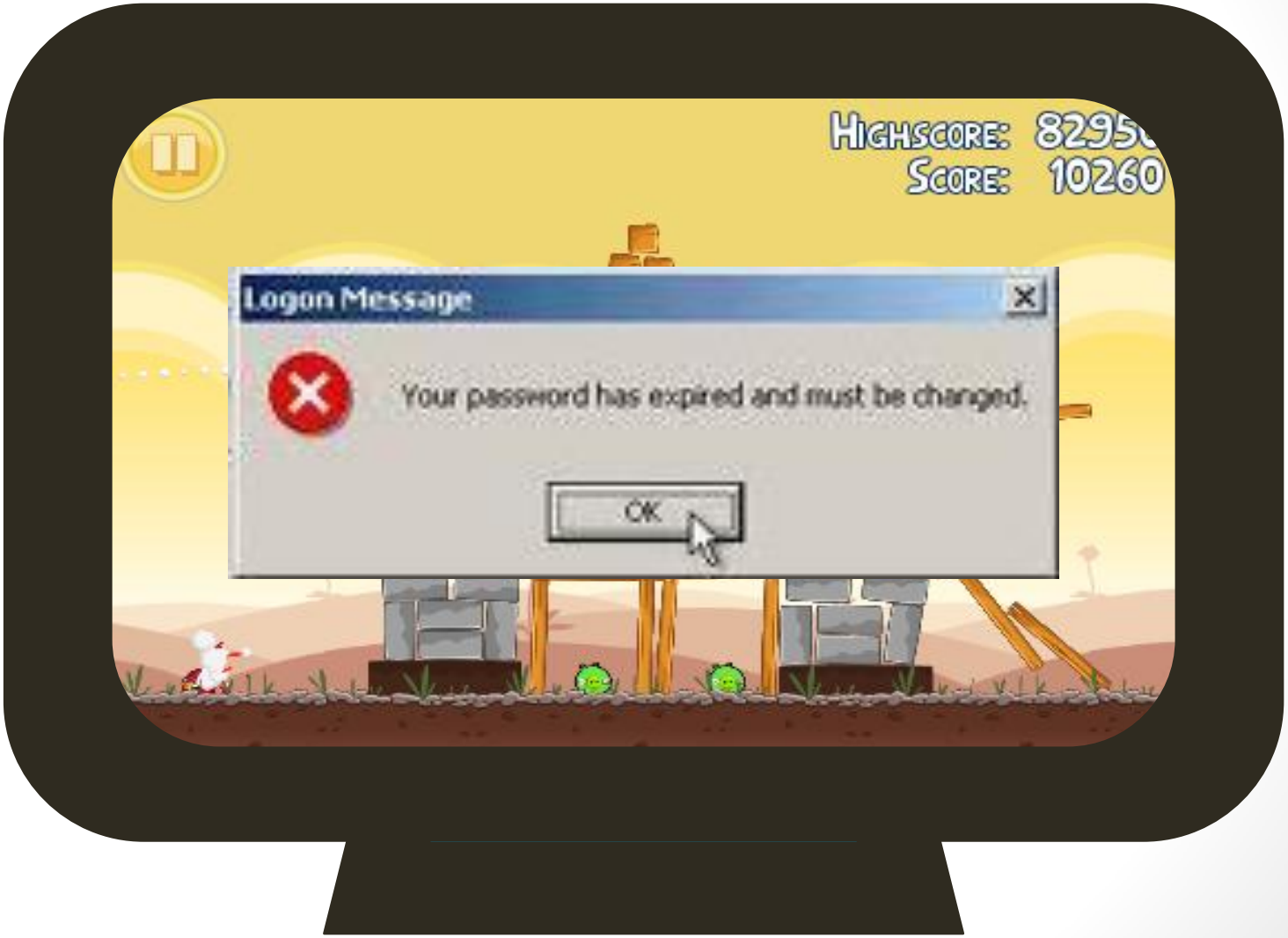
A new game: SkipIt



- With more information, this game is much simpler to analayze!

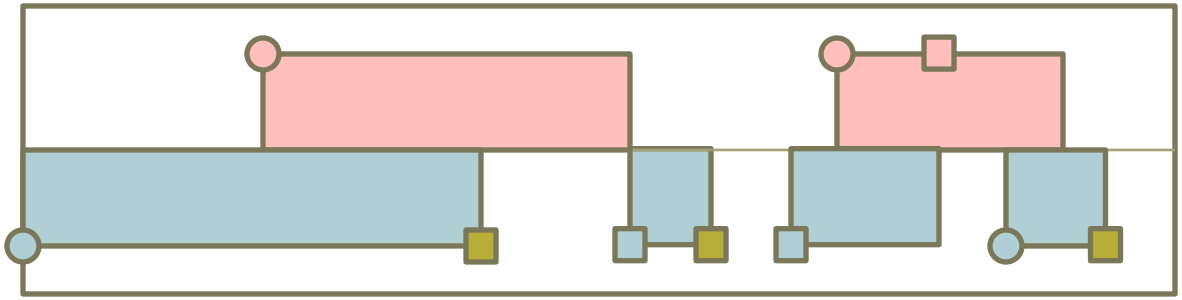
- Situation: We don't have access
  - Strategy: depends on opponent's strategy for lock downs
- Situation: We have access
  - Strategy: we are benefitting, why pay?
- Theorem 1: Nash equilibrium: Share, Man!

Lorem Ipsum Deserta Omnia



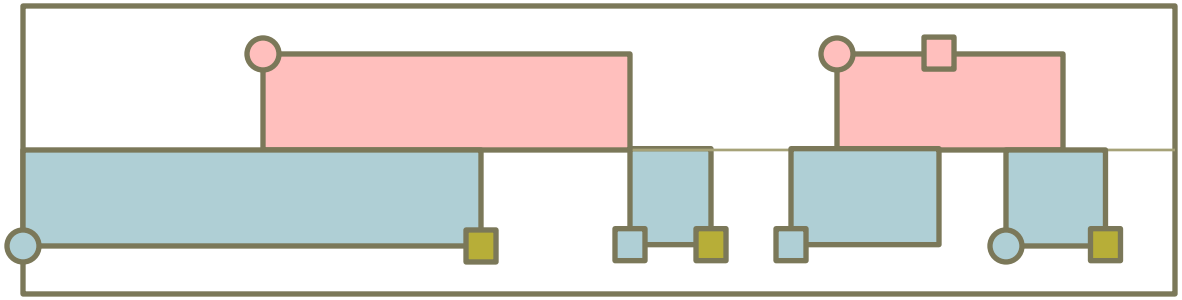
Lorem Ipsum Deserta Omnia

(information technology ruins everything)



- Three player game
  - attacker, defender,
  - defender's IT department
- IT's goal is to *minimize* attacker's benefit
- IT has one kind of move (with no cost): bother the defender to do a lock-down.
  - Defender's benefit ceases until they lock down.
  - Defender, but not attacker, aware of bothering.

3-player game: `FlipITOff`



- Defender strategy:
  - Obtain access when necessary.
  - Use adaptive `FlipIt` strategy against IT's bothering strategy to determine lock downs.
- Attacker strategy:
  - Play `FlipIt` against Defender's lock down strategy
  - Never lock down.
- IT strategy:
  - Bother Defender in order to maximize frequency of defender lock downs
- Theorem 2: Equilibrium maximally painful for defender.