TECHNISCHE UNIVERSITÄT DRESDEN

Department of Computer Science Institute of System Architecture, Operating Systems Group

THE MATHEMATICS OF OBSCURITY

HERMANN HÄRTIG,
CLAUDE-JOACHIM HAMANN,
MICHAEL ROITZSCH

DISCLAIMER

I will tell about...

- the process of finding **security errors**
- our **mathematical model** for it
- the **comparison** of open and closed source

I will not tell about...

- whether open or closed source is **better**

BATTLE ROYALE

Open Source | **Closed Source**

TECHNISCHE UNIVERSITÄT DRESDEN

BATTLE ROYALE

Open Source	Closed Source
everyone has access to source code	only the company has the source code
everyone can search for bugs	attackers have a harder time
more defenders find more bugs	bugs are prevented from being exploited
easier to find bugs	harder to find bugs

PROPOSITION

Attackers only need only one error.
Defenders need to find all errors.

MODEL

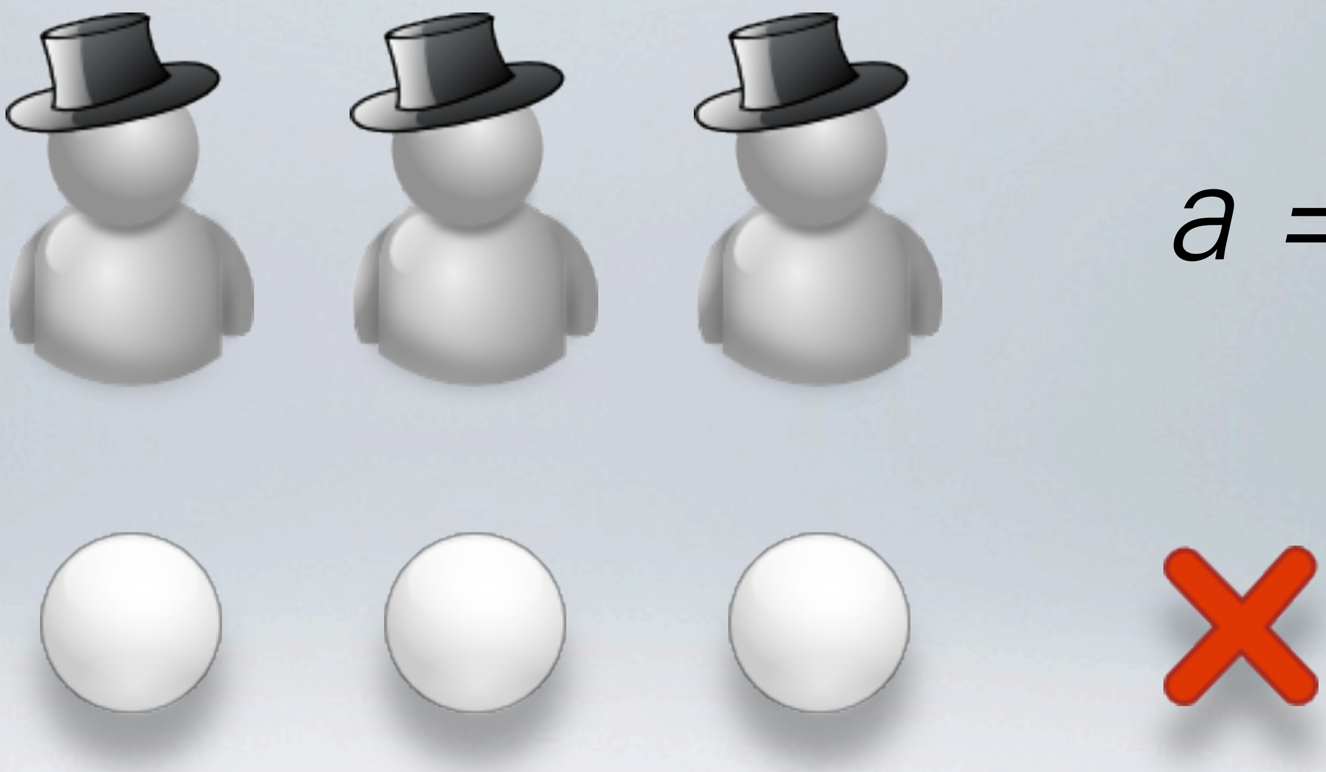
3 Errors:

No Error:

$e = 3$

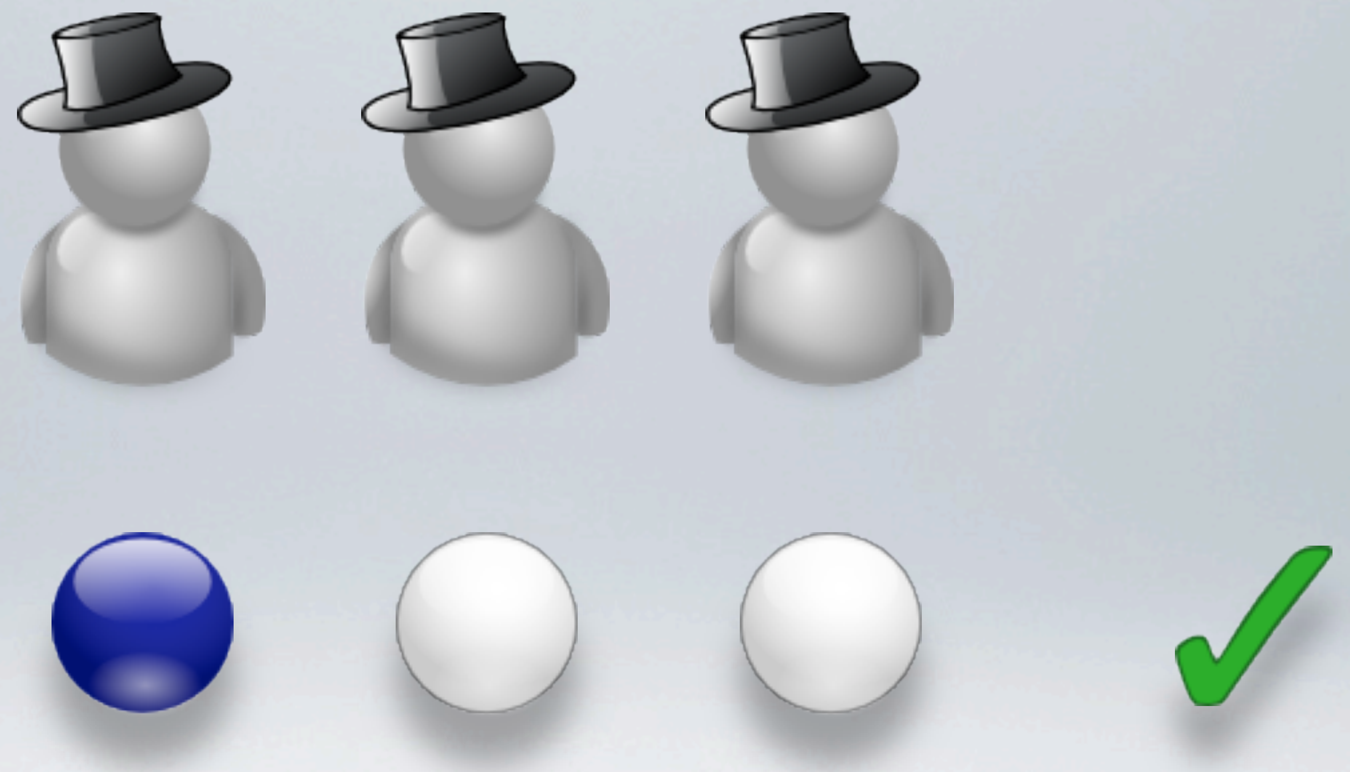
p, q

ATTACKERS



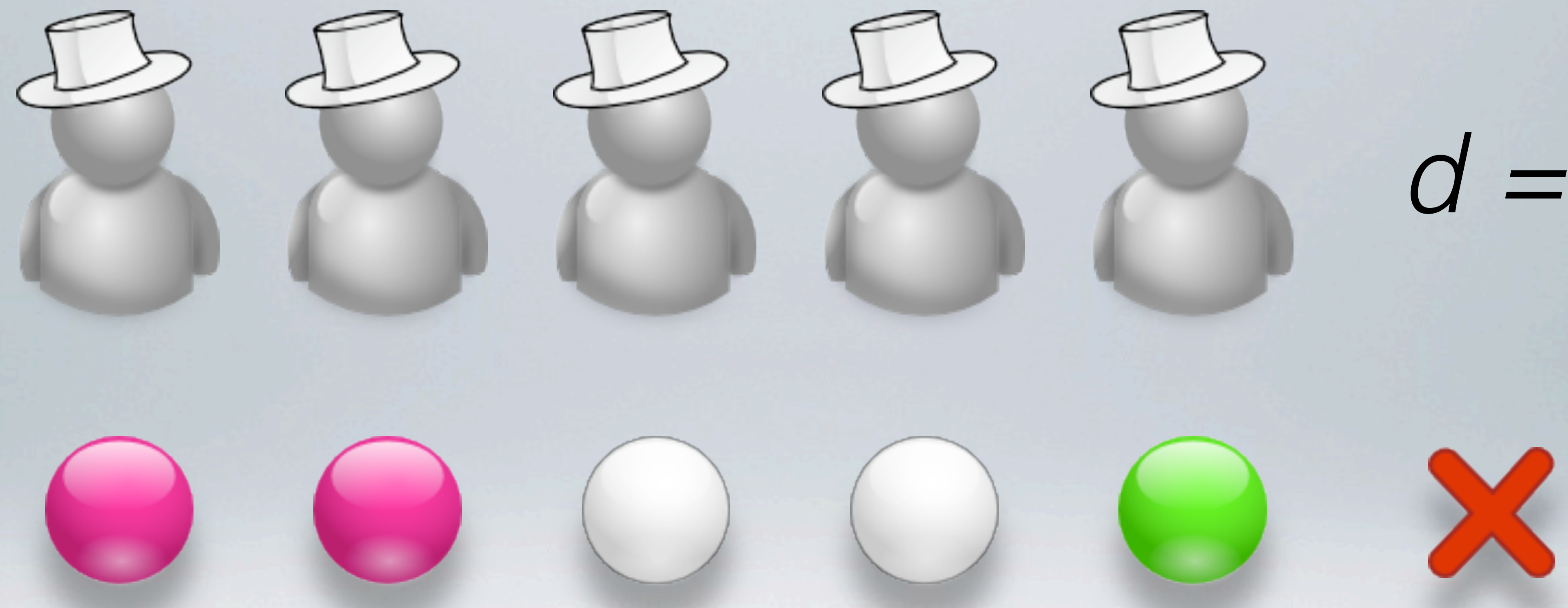
$a = 3$

ATTACKERS



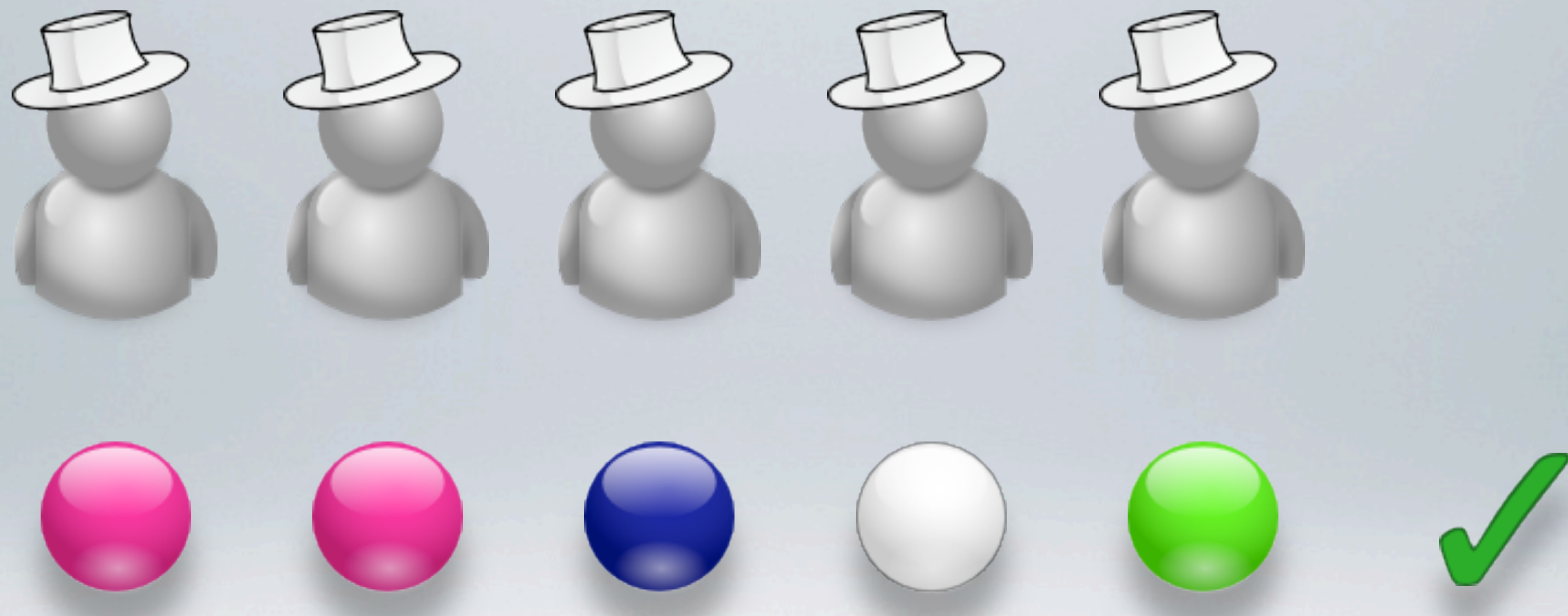
$$\boxed{p_A = 1 - (1 - ep)^a}$$

DEFENDERS



$d = 5$

DEFENDERS



$$p_D = e! \cdot \sum_{i=0}^{d-e} \binom{d}{i} q^{d-i} \left(1 - eq\right)^i S_{d-i,e}$$

EXAMPLE

- 20 errors

$$e = 20$$

- 1% probability to find an error

$$p = q = 0.01$$

- 75% desired winning chance

$$p_A = p_D = 0.75$$

- How many attackers?

$$a = 7$$

- How many defenders?

$$d = 424$$

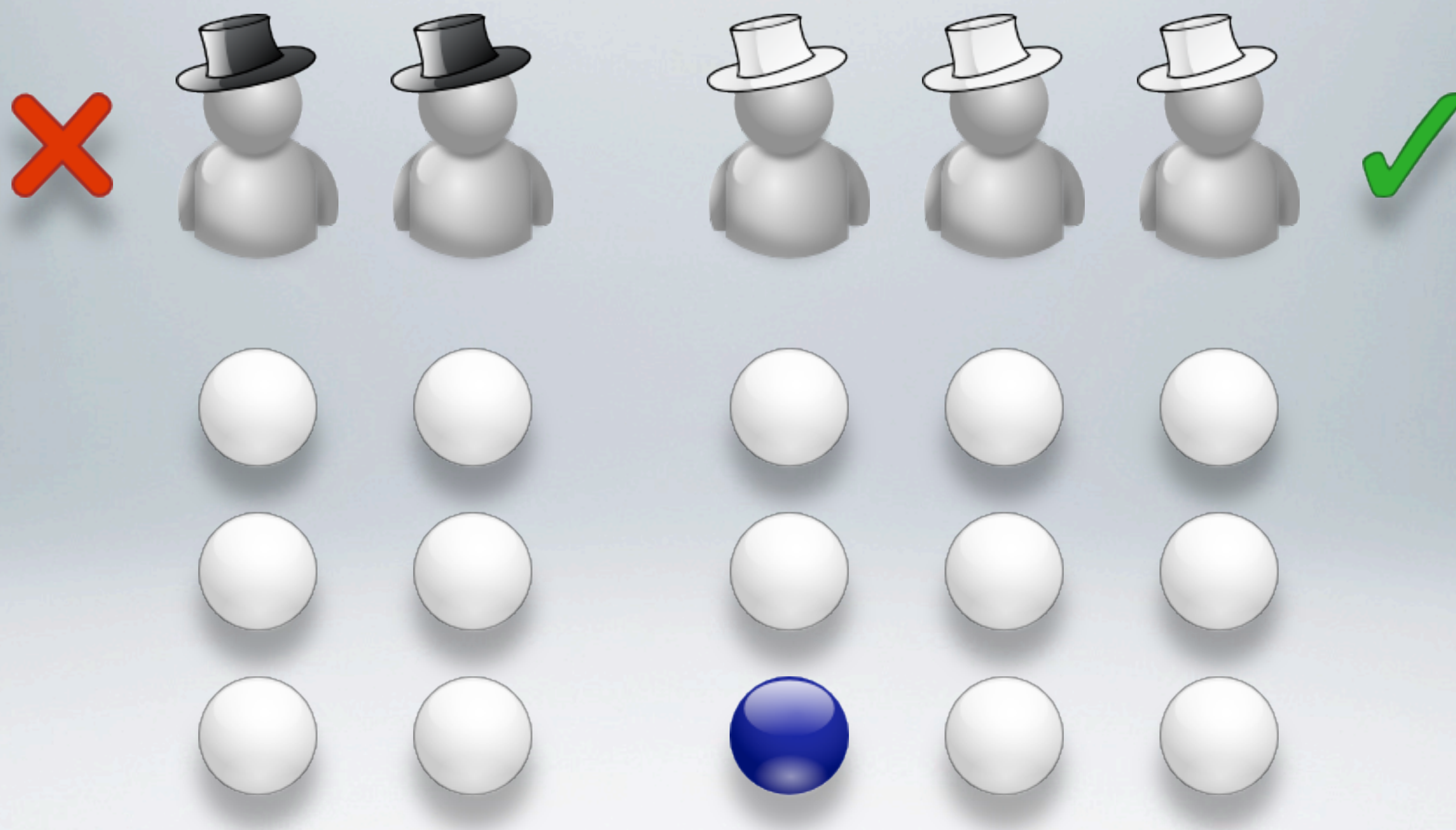
FLAWS

- What happens if both sides lose?
- … or win?
- Do the defenders really lose if they do not find all errors?
- They just have to find the errors **first**.
- Instead of a snapshot, model a **race**.

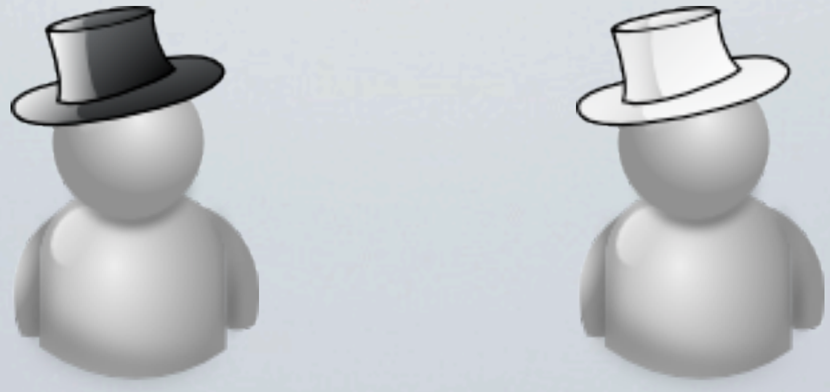
PROPOSITION

Defenders need to find any error earlier than the attackers.

RACE



PROBABILITY



p — *m* steps

q — *n* steps

$$p_{m,n} = (1-p)^{m-1}\,p \cdot (1-q)^{n-1}\,q$$

PROBABILITY

$$\boxed{p_{m,n} = (1-p)^{m-1}\, p \cdot (1-q)^{n-1}\, q}$$

defenders win for $n < m$

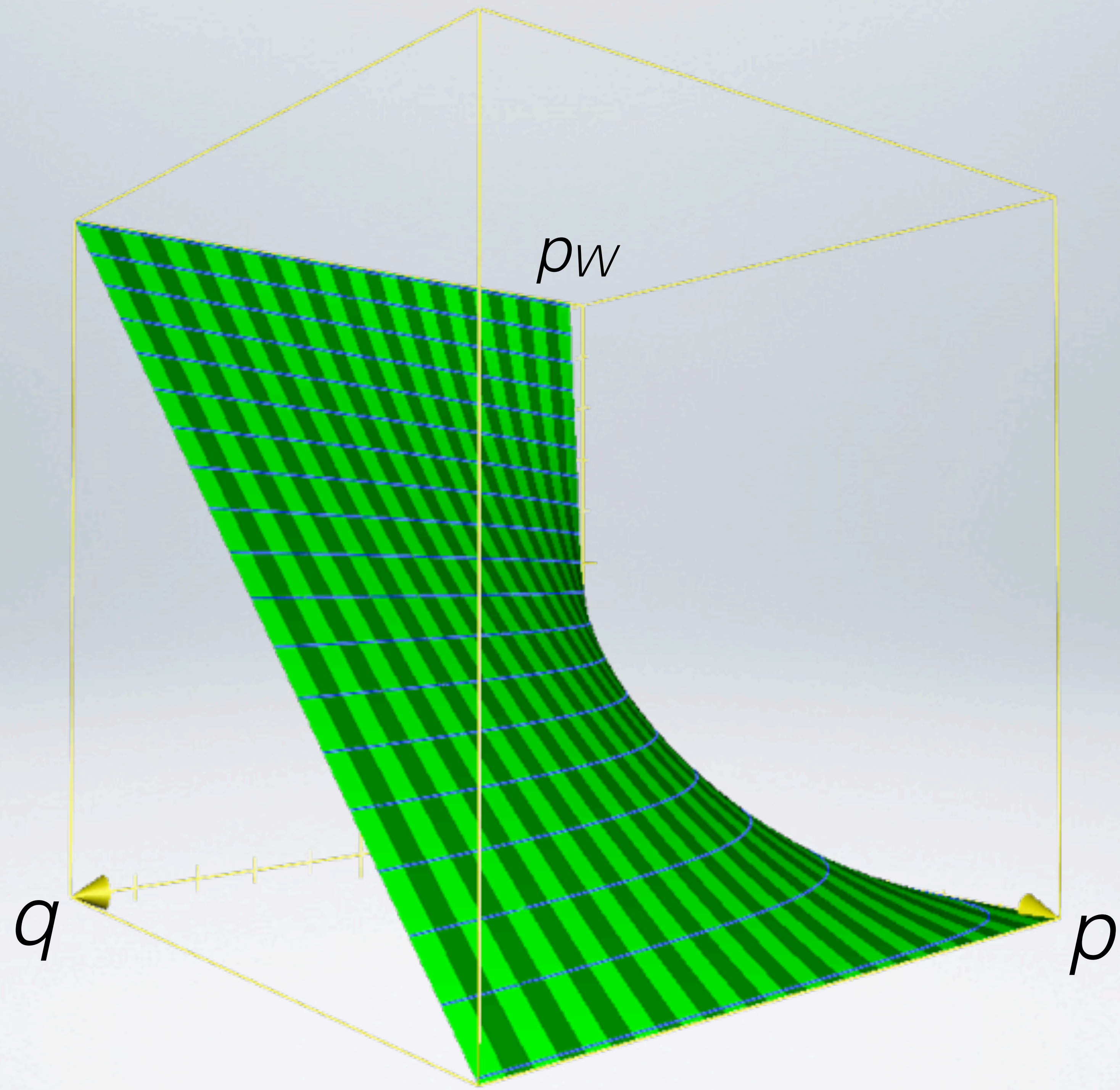
$$\boxed{p_W = \sum_{n=1}^{\infty} \sum_{m=n+1}^{\infty} p_{m,n} = \frac{q\,(1-p)}{q\,(1-p)+p}}$$

PROBABILITY

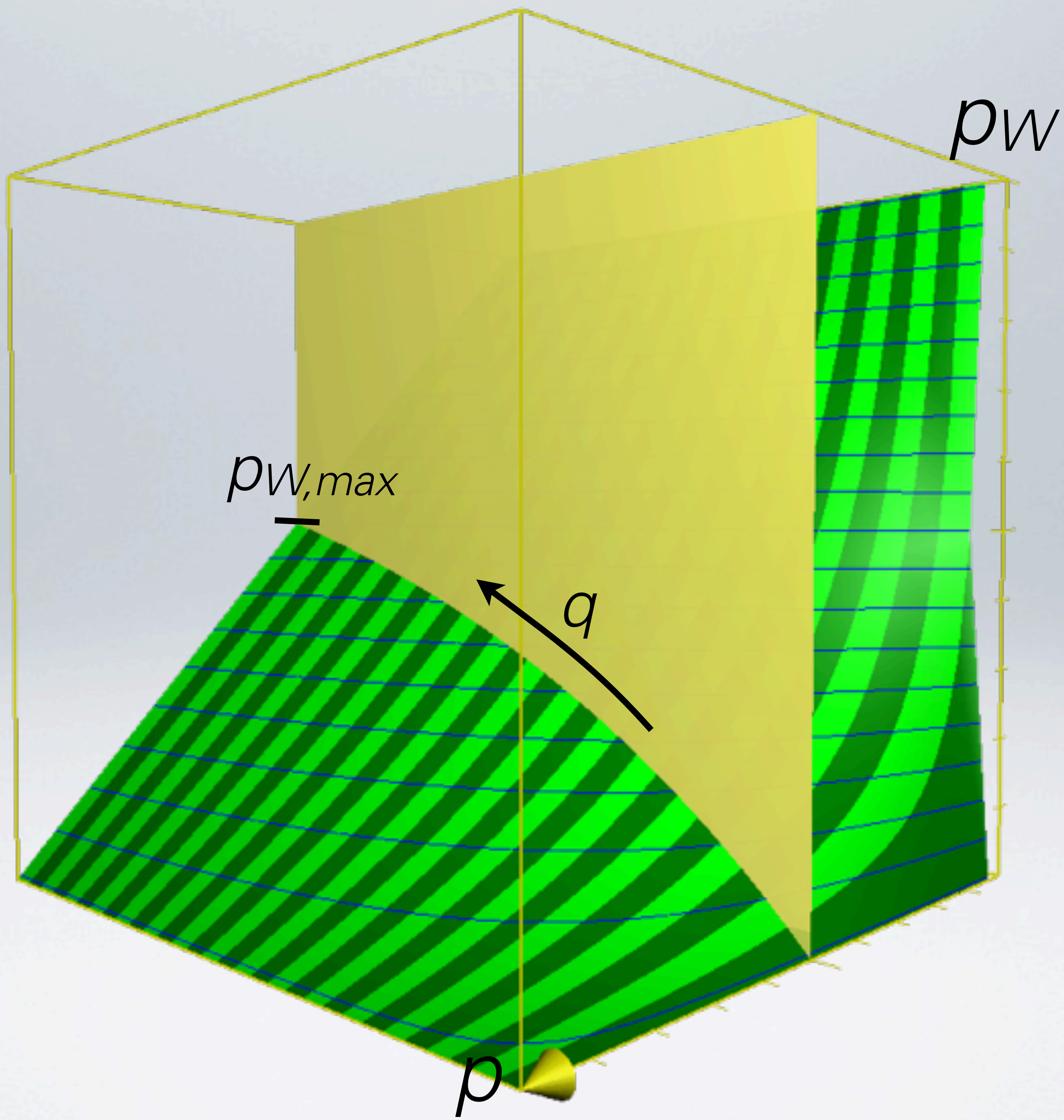
$$p_W = \sum_{n=1}^{\infty} \sum_{m=n+1}^{\infty} p_{m,n} = \frac{q\,(1-p)}{q\,(1-p)+p}$$

open source	more defenders	higher q
closed source	harder for attackers	lower p

GRAPH



GRAPH



EXAMPLE

- 1 million lines of code, 15 security errors
  $e = 15$
- probability for a single defender to find an error
  $q_{single} = 0.002\%$
- the same for attackers in open source case
  $p_{single,open} = 0.002\%$
- closed source factor 2 harder
  $p_{single,closed} = 0.001\%$
- 500 attackers
- How many defenders do we need?

TECHNISCHE UNIVERSITÄT DRESDEN

RESULTS

	pw = 0.6	pw = 0.9
closed source	7815	62088
open source	17133	impossible

CONCLUSION

No matter how many defenders, there's always a window for attackers.

SUMMARY

- urn model for discovery of security errors
- race between attackers and defenders
- there is an upper bound for the defenders
- this bound may be hit in reality