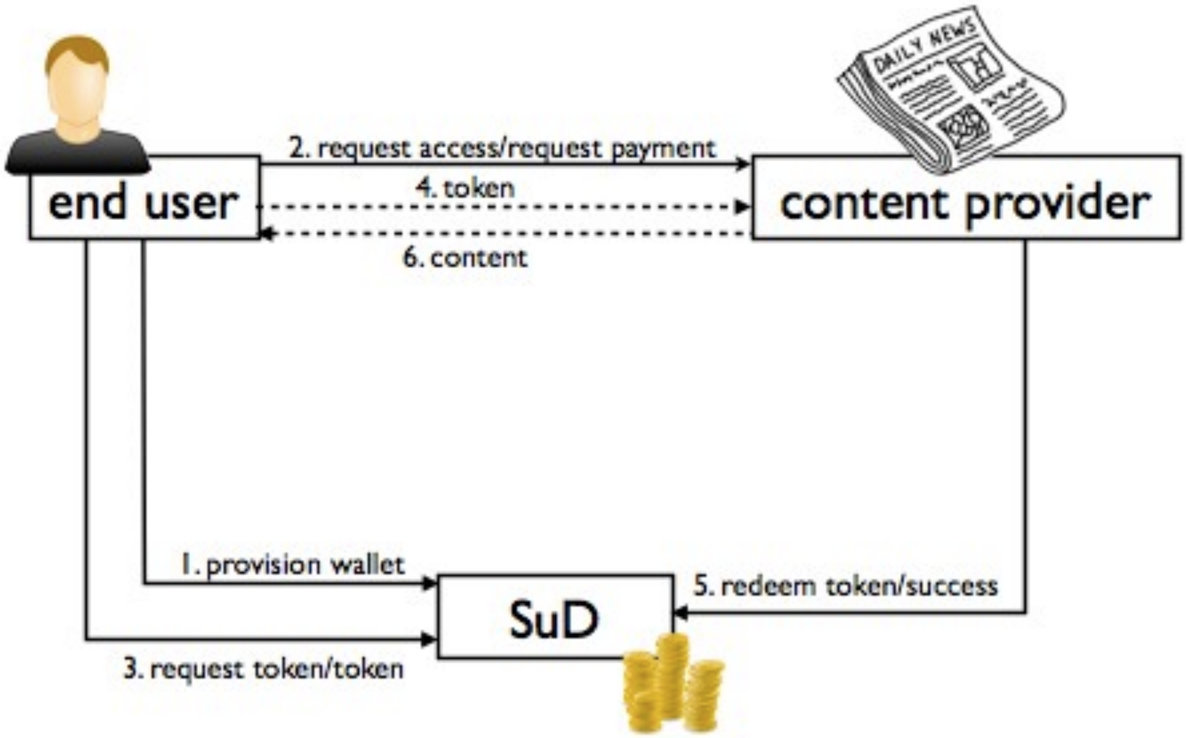
# threat modeling

Johan Peeters
http://johanpeeters.com
yo@johanpeeters.com

## me

- independent software architect
- nearshoring
  - software
  - software as a service
- secappdev.org founder
- active in agile community

# case study



end user

content provider

SuD

2. request access/request payment

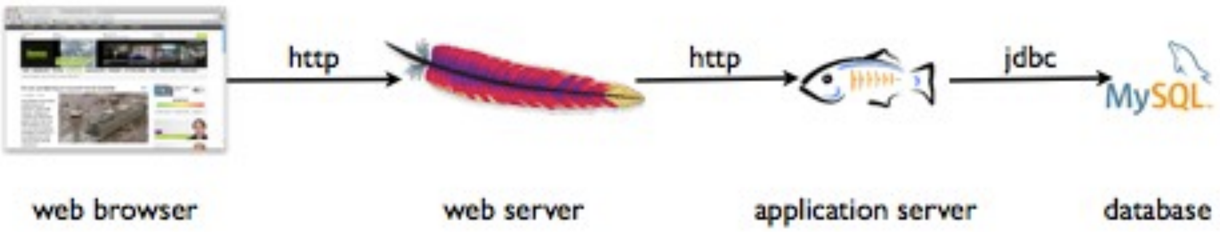
4. token

6. content

1. provision wallet

3. request token/token

5. redeem token/success



web browser

http

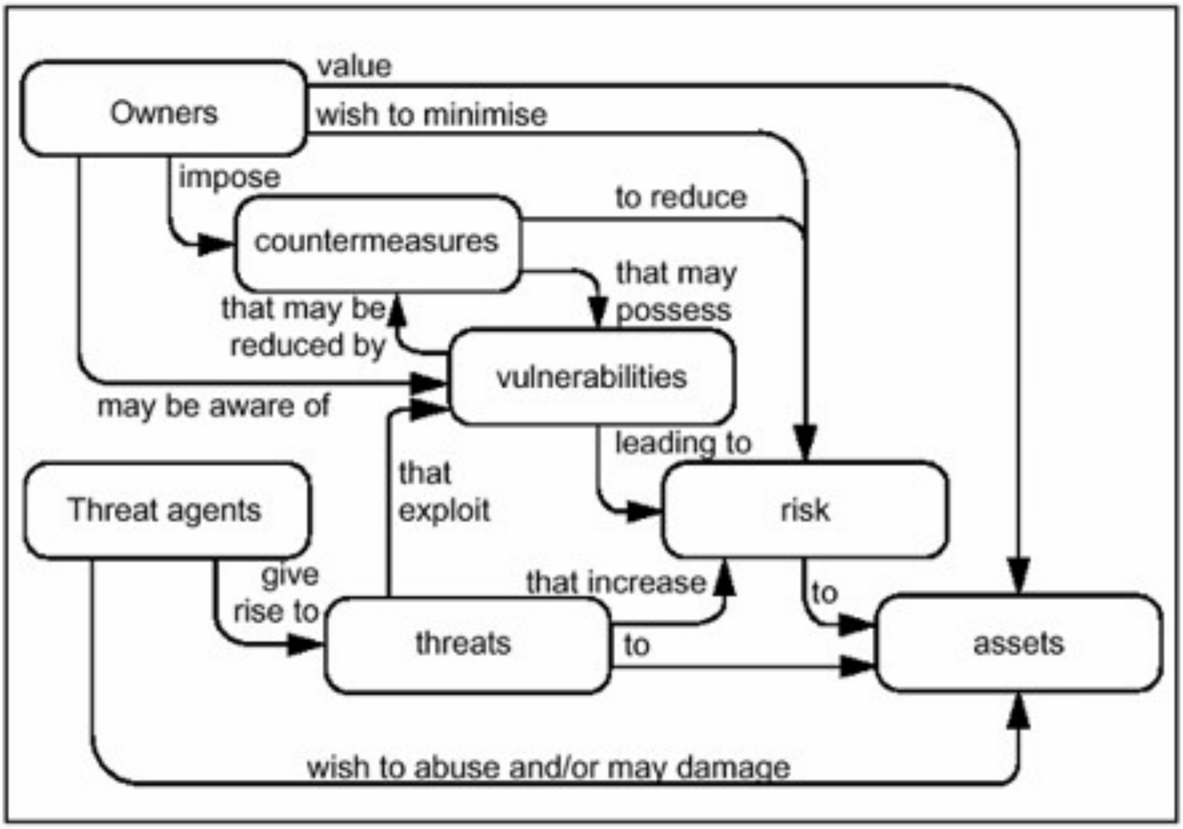
web server

http

application server

jdbc

database



Owners

value

wish to minimise

impose

countermeasures

to reduce

that may possess

that may be reduced by

vulnerabilities

may be aware of

leading to

Threat agents

that exploit

risk

give rise to

threats

that increase

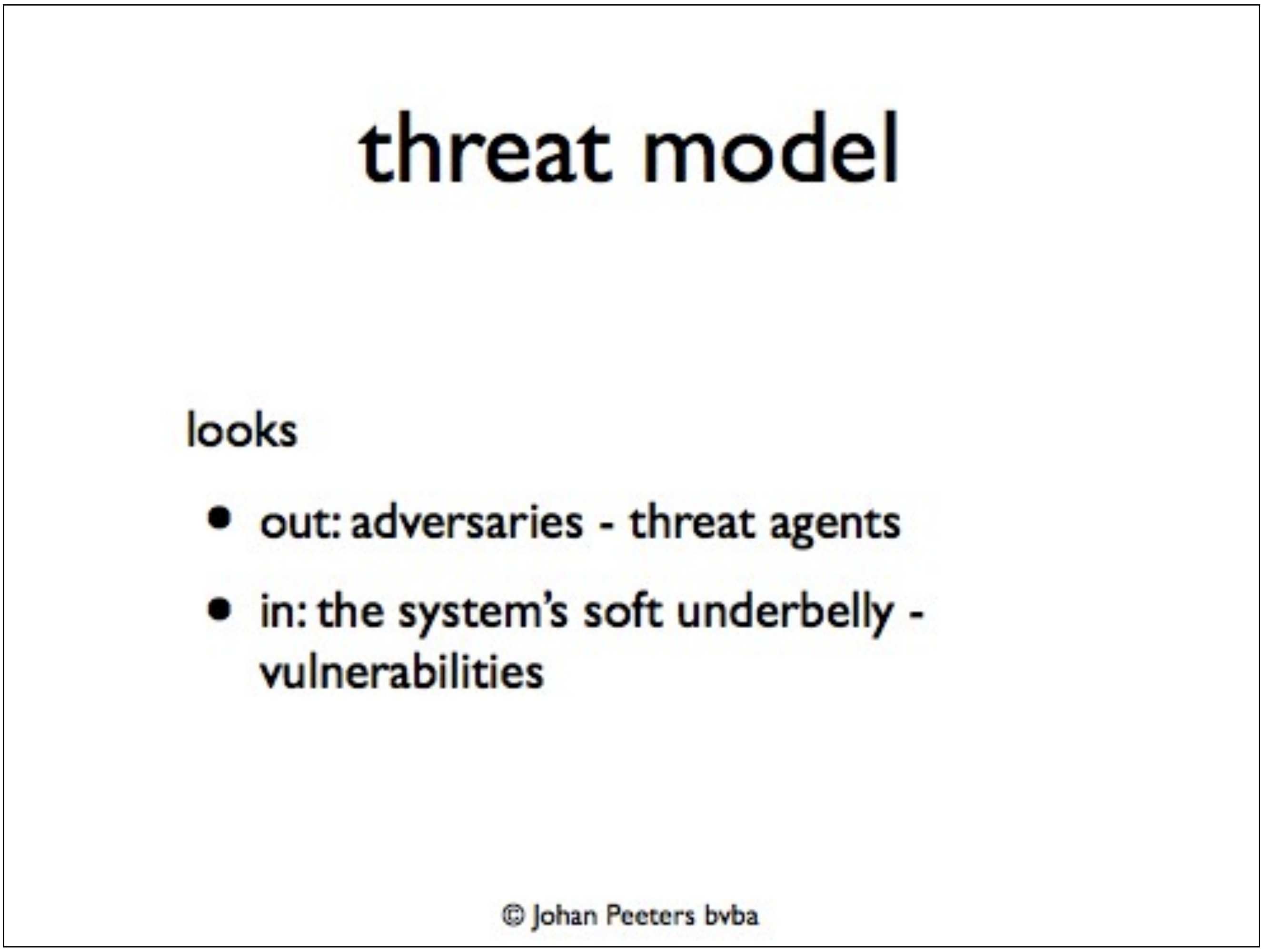
to

to

assets

wish to abuse and/or may damage

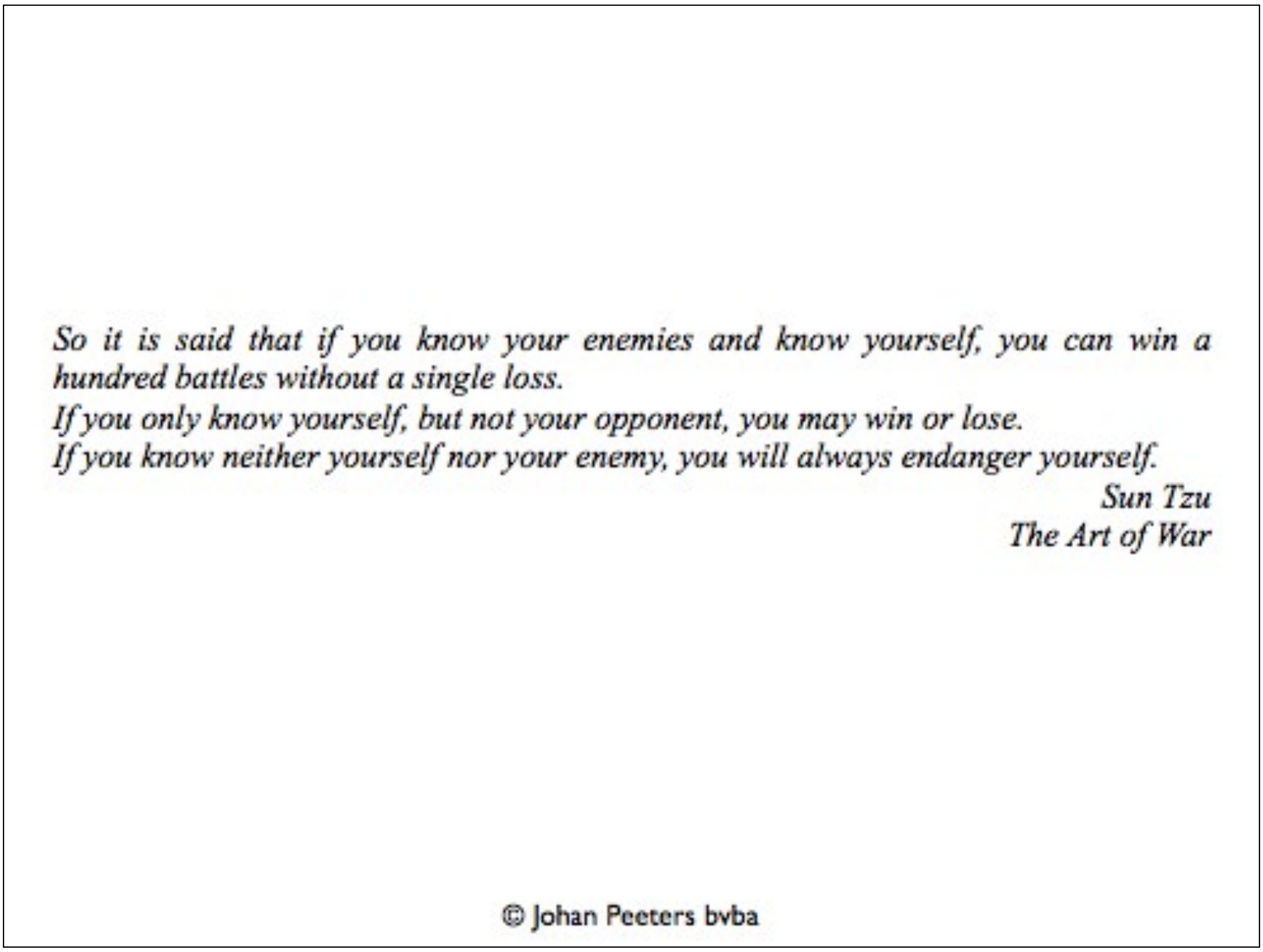
from the Common Criteria part 1 version 2



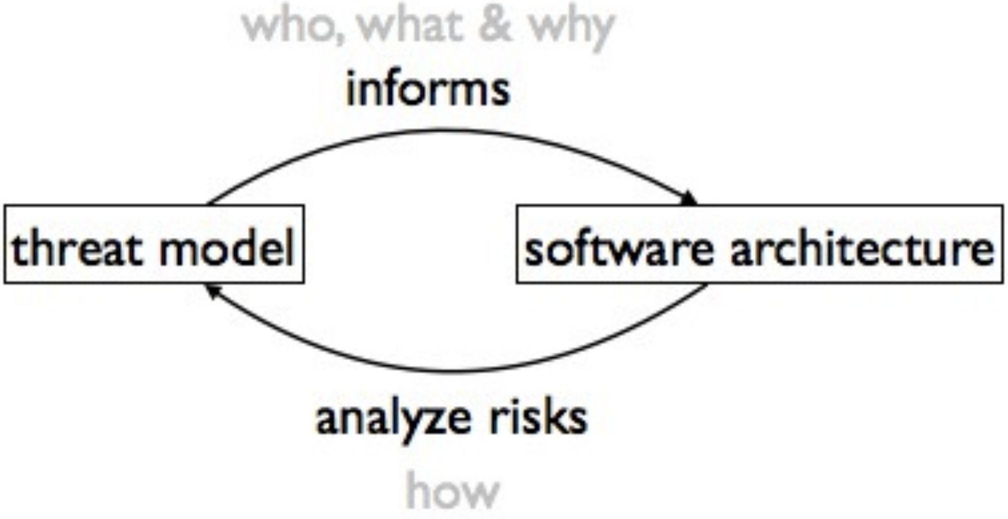
# threat model

looks

- out: adversaries - threat agents
- in: the system's soft underbelly - vulnerabilities



> *So it is said that if you know your enemies and know yourself, you can win a hundred battles without a single loss.*
> *If you only know yourself, but not your opponent, you may win or lose.*
> *If you know neither yourself nor your enemy, you will always endanger yourself.*
>
> *Sun Tzu*
> *The Art of War*



# assignment 1

- who are the potential adversaries?
- what targets/assets are they after?
- for each asset, specify the critical protection properties, e.g.
  - confidentiality
  - integrity
  - availability

**timebox: 10 mins**

# format output

| adversaries | targets | |
|---|---|---|
| end user | content | confidentiality |
| | | integrity |
| | account | integrity |
| content provider | value of token | integrity |

# assignment 2

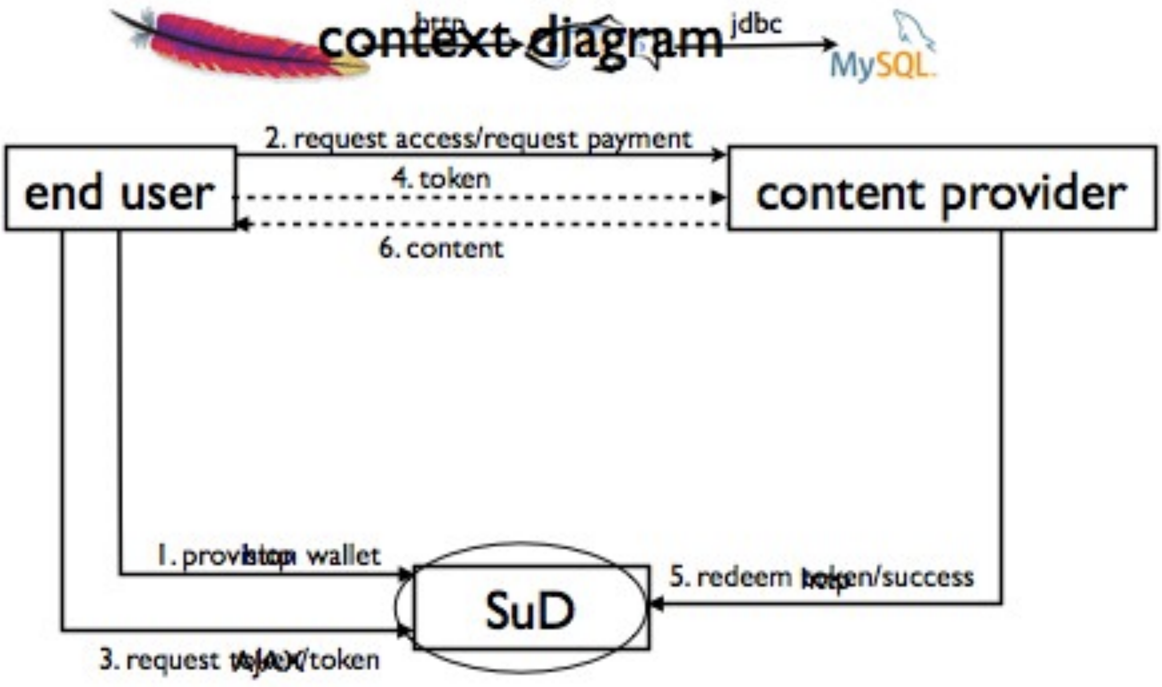
- for each adversary
    - for each goal achieved
        - estimate value to the adversary
        - estimate damage to us

**timebox: 10 mins**

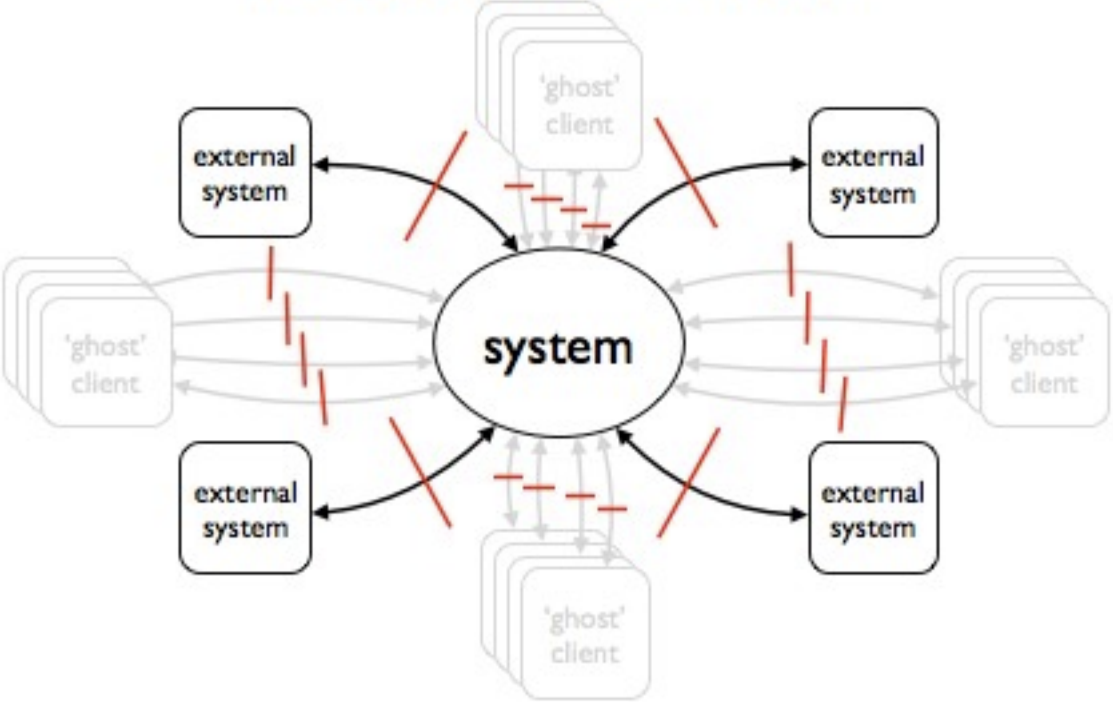
# format output

| adversaries | targets | | value | damage |
|---|---|---|---|---|
| end user | content | confidentiality | 1 | 5 |
| | | integrity | 1 | 5 |
| | account | integrity | 3 | 8 |
| content provider | value of token | integrity | 8 | 8 |

# context diagram

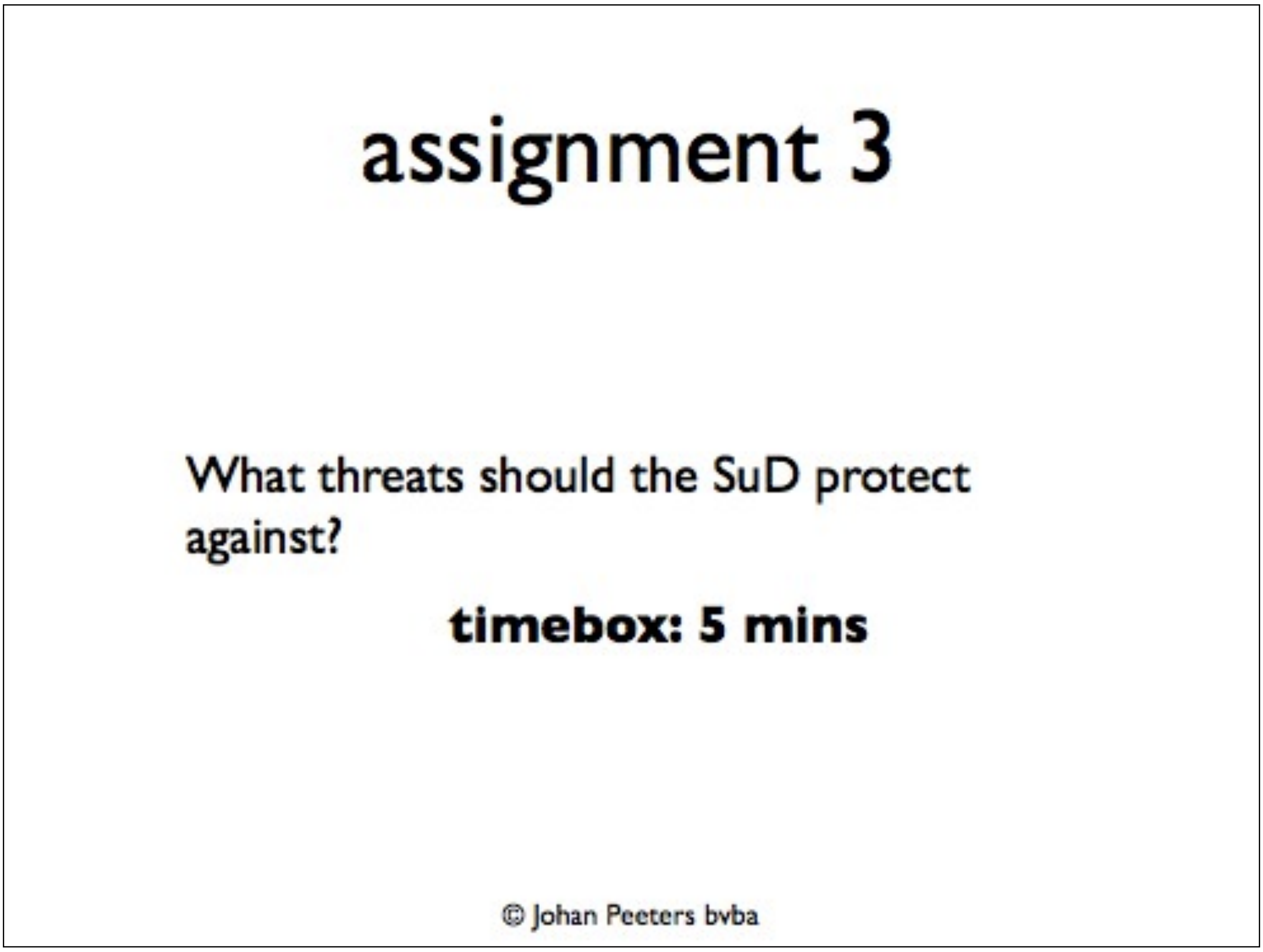


# attack surface



# attack surface

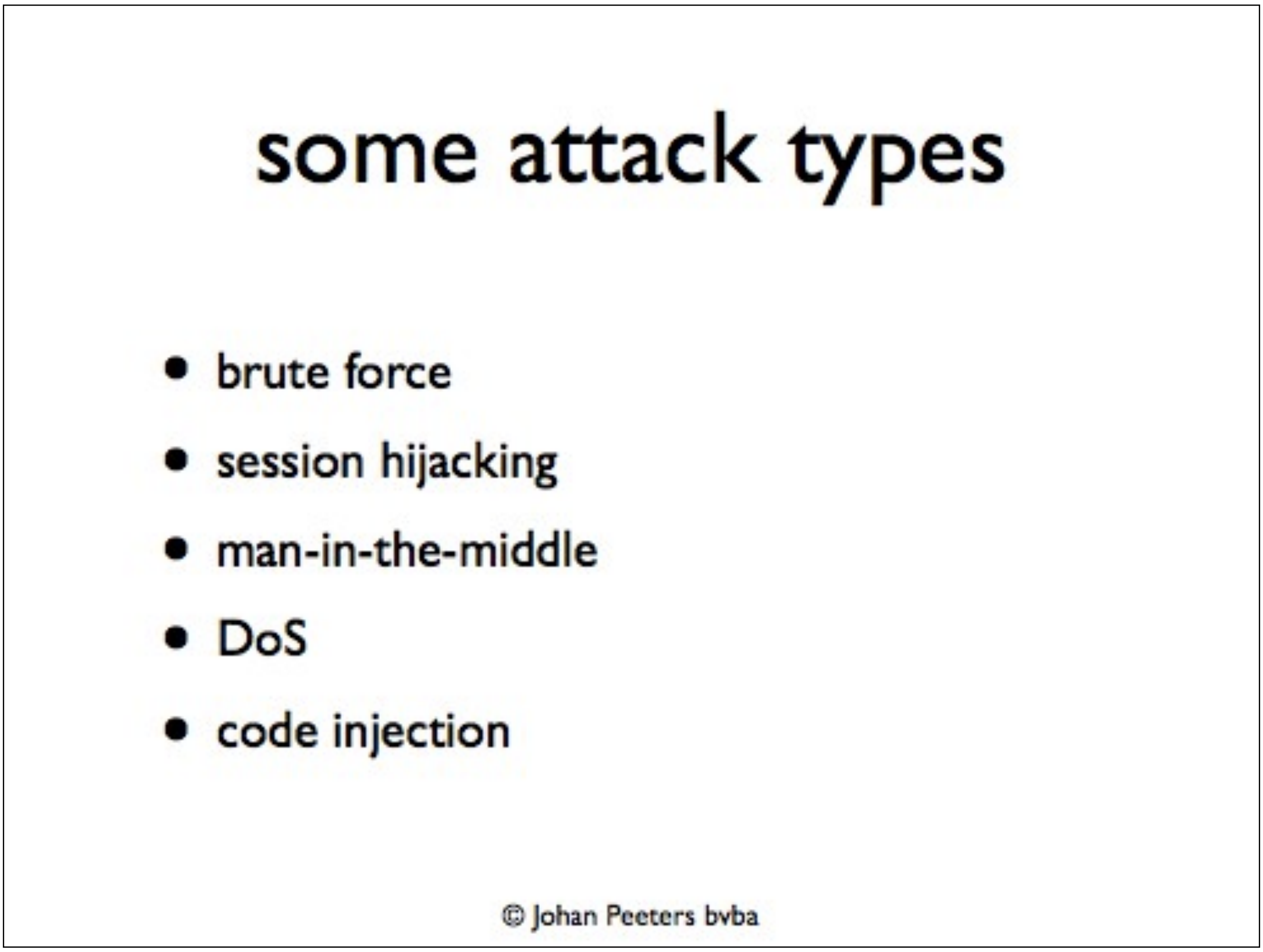
- system exposes interfaces to its environment - entry points
  - intentional
  - unintentional
    - included in third-party components
    - side-channels
- each interface presents an opportunity to an adversary for abuse



# assignment 3

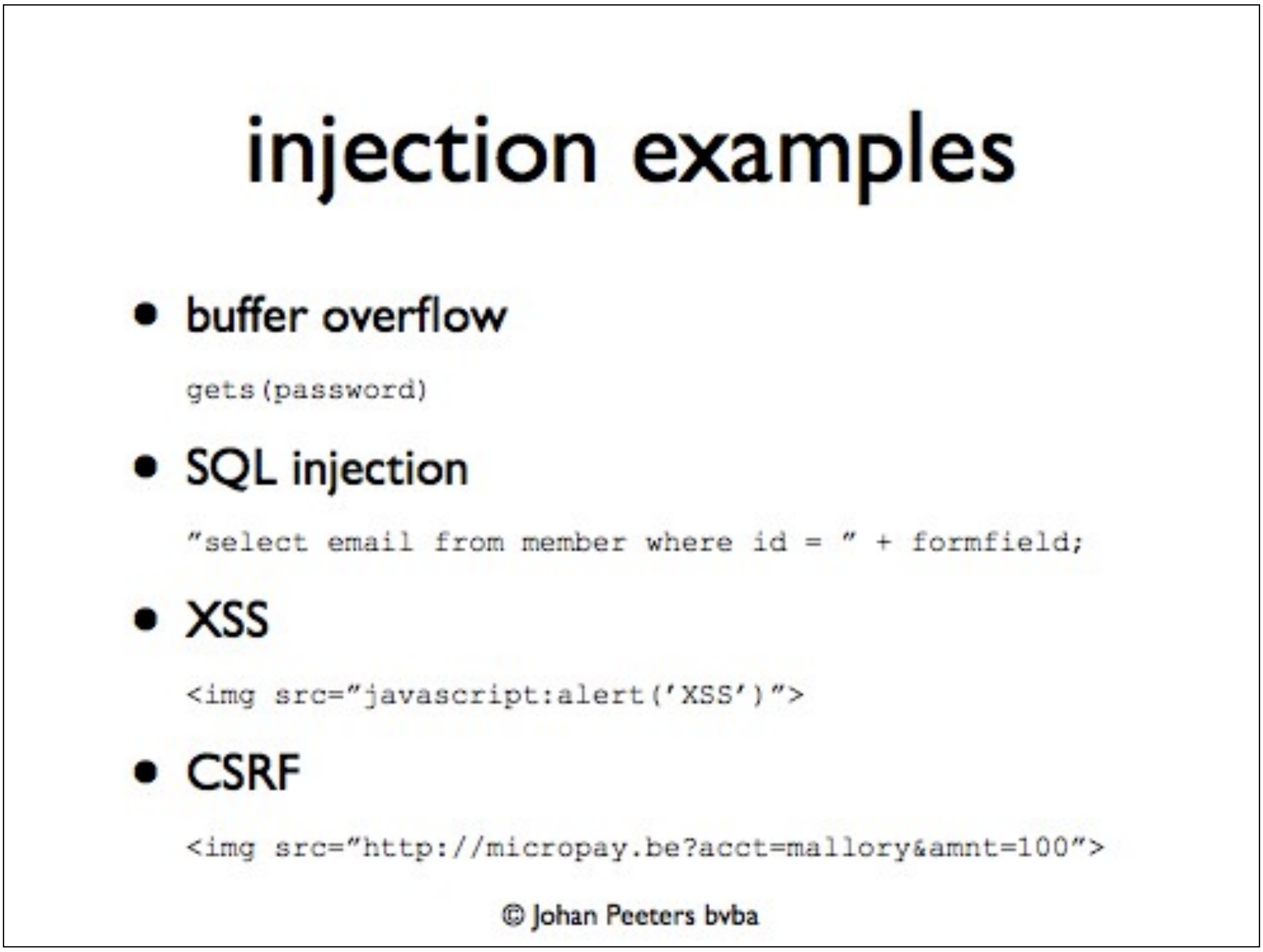
What threats should the SuD protect against?

**timebox: 5 mins**



# some attack types

- brute force
- session hijacking
- man-in-the-middle
- DoS
- code injection



# injection examples

- buffer overflow

```
gets(password)
```

- SQL injection

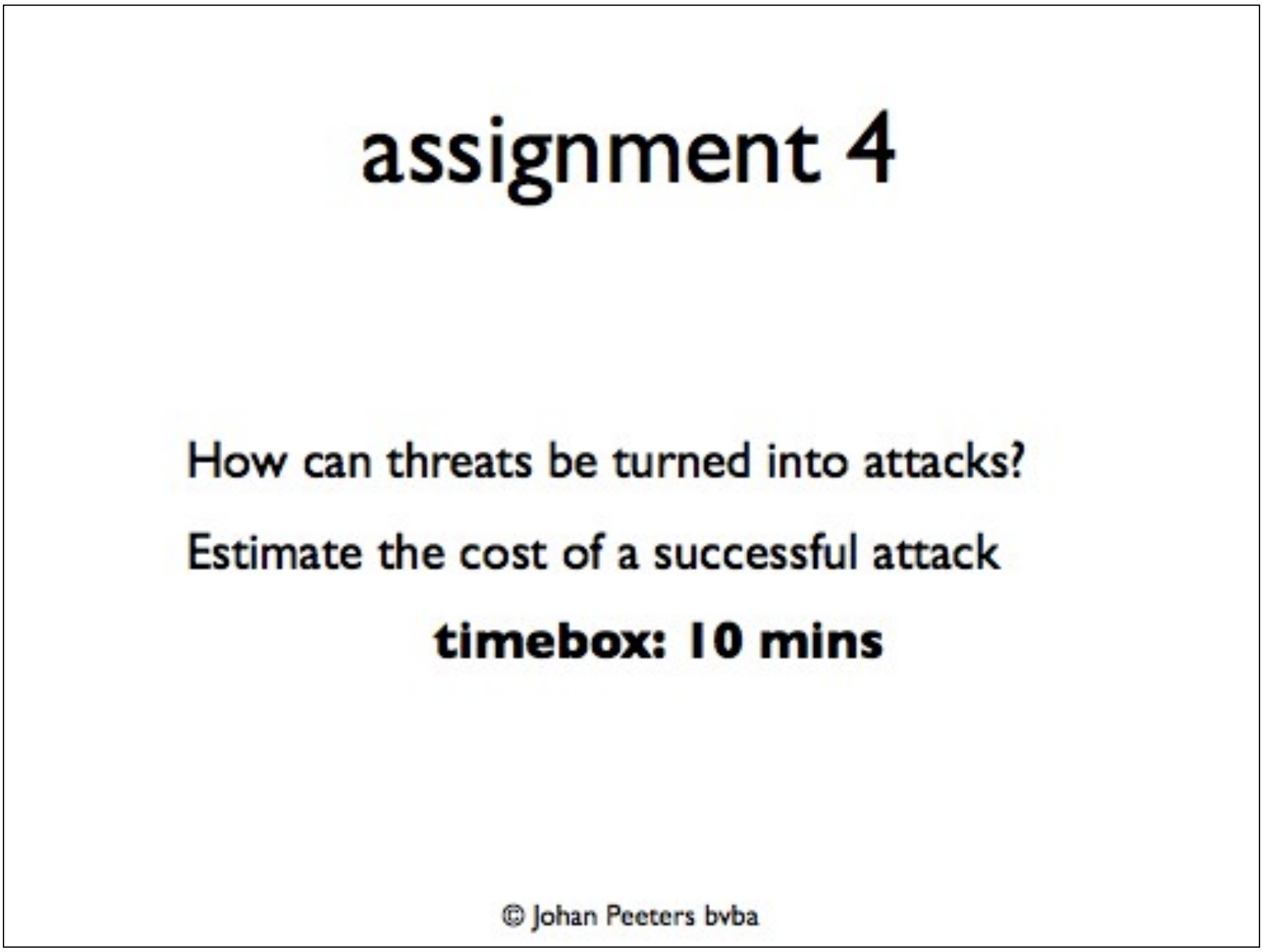
```
”select email from member where id = ” + formfield;
```

- XSS

```
<img src=”javascript:alert(’XSS’)”>
```

- CSRF

```
<img src=”http://micropay.be?acct=mallory&amnt=100”>
```

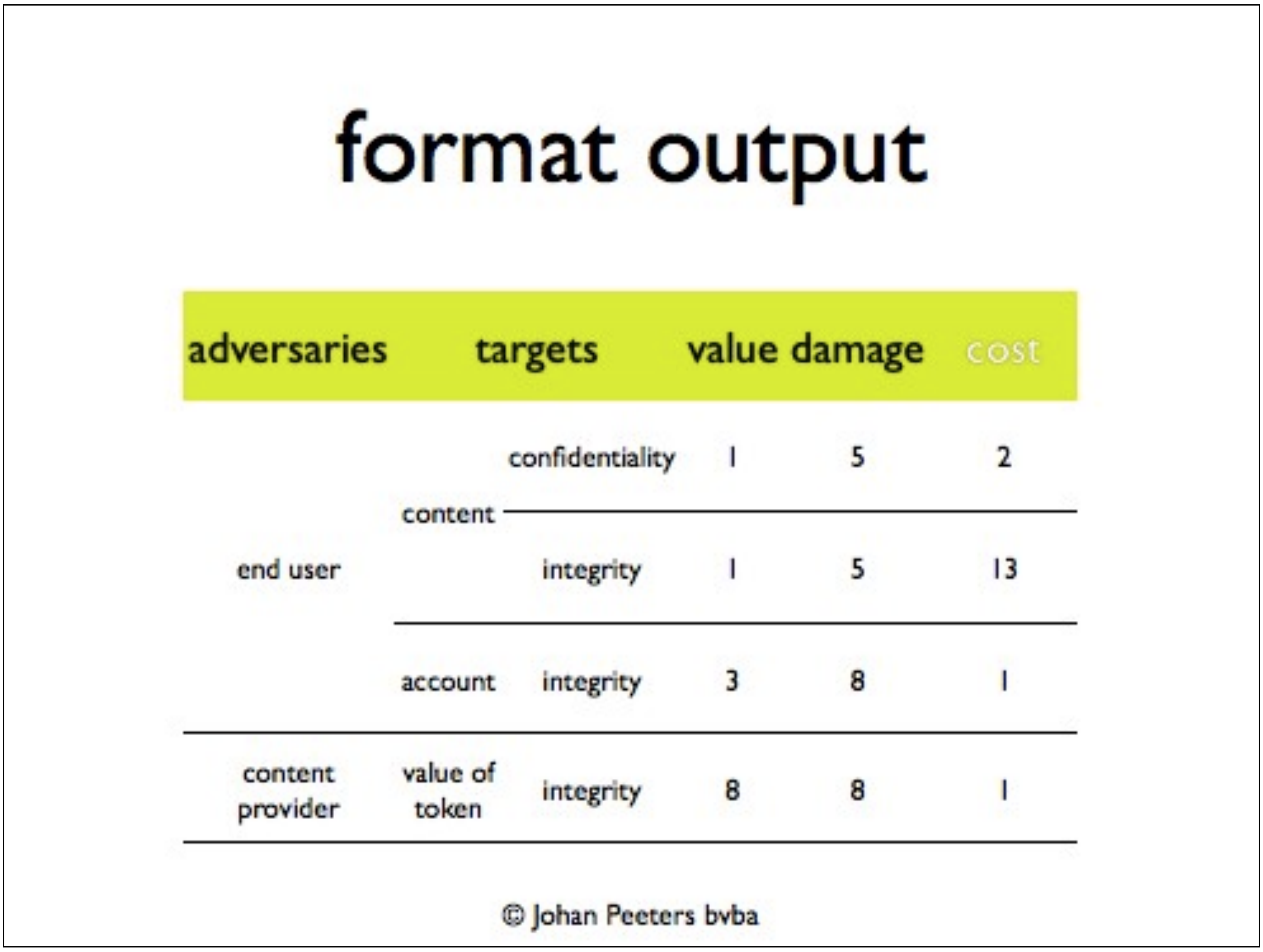


# assignment 4

How can threats be turned into attacks?

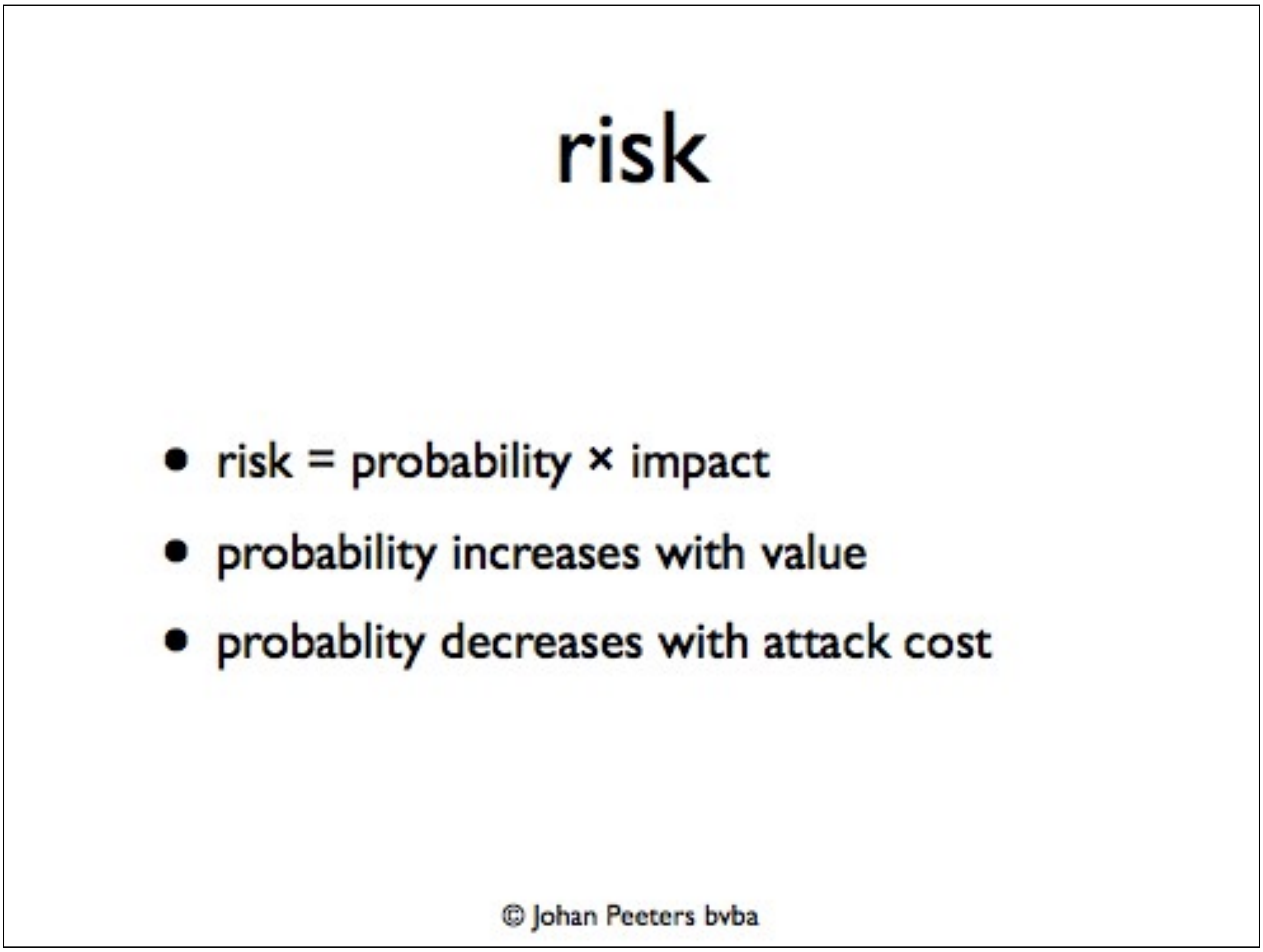
Estimate the cost of a successful attack

**timebox: 10 mins**



# format output

| adversaries | targets | | value | damage | cost |
|---|---|---|---|---|---|
| end user | content | confidentiality | 1 | 5 | 2 |
| | | integrity | 1 | 5 | 13 |
| | account | integrity | 3 | 8 | 1 |
| content provider | value of token | integrity | 8 | 8 | 1 |



# risk

- risk = probability × impact
- probability increases with value
- probablity decreases with attack cost

# assignment 5

rank the risks

**timebox: 5 mins**

# format output

| adversaries | targets | | value | damage | cost | risk ranking |
|---|---|---|---|---|---|---|
| end user | content | confidentiality | 1 | 5 | 2 | 3 |
| | | integrity | 1 | 5 | 13 | 4 |
| | account | integrity | 3 | 8 | 1 | 2 |
| content provider | value of token | integrity | 8 | 8 | 1 | 1 |

# assignment 6

which risk should we

- externalize?
- absorb?
- mitigate with procedural controls?
- mitigate with technical measures?

**timebox: 10 mins**

☑ threat model

□ risk mitigation strategies

□ work items