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

© Johan Peeters bvba
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

<table>
<thead>
<tr>
<th>adversaries</th>
<th>targets</th>
</tr>
</thead>
<tbody>
<tr>
<td>end user</td>
<td>confidentiality</td>
</tr>
<tr>
<td></td>
<td>content</td>
</tr>
<tr>
<td></td>
<td>integrity</td>
</tr>
<tr>
<td>account</td>
<td>integrity</td>
</tr>
<tr>
<td>content provider</td>
<td>value of token</td>
</tr>
<tr>
<td></td>
<td>integrity</td>
</tr>
</tbody>
</table>

© Johan Peeters bvba

assignment 2

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

  timebox: 10 mins

© Johan Peeters bvba
## format output

<table>
<thead>
<tr>
<th>adversaries</th>
<th>targets</th>
<th>value</th>
<th>damage</th>
</tr>
</thead>
<tbody>
<tr>
<td>confidentiality</td>
<td>content</td>
<td>1</td>
<td>5</td>
</tr>
<tr>
<td>end user</td>
<td>integrity</td>
<td>3</td>
<td>8</td>
</tr>
<tr>
<td>account</td>
<td>integrity</td>
<td>8</td>
<td>8</td>
</tr>
<tr>
<td>content provider</td>
<td>value of token</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>integrity</td>
<td>3</td>
<td>8</td>
</tr>
</tbody>
</table>

© Johan Peeters bvba

---

## context diagram

1. provide wallet
2. request access/request payment
3. request token
4. token
5. redeem token/success
6. content
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

© Johan Peeters bvba
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">`

© Johan Peeters bvba

assignment 4

How can threats be turned into attacks?
Estimate the cost of a successful attack

**timebox: 10 mins**
format output

<table>
<thead>
<tr>
<th>adversaries</th>
<th>targets</th>
<th>value damage</th>
<th>cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>confidentiality</td>
<td>1</td>
<td>5</td>
<td>2</td>
</tr>
<tr>
<td>content</td>
<td>end user</td>
<td>integrity</td>
<td>1</td>
</tr>
<tr>
<td>account</td>
<td>integrity</td>
<td>3</td>
<td>8</td>
</tr>
<tr>
<td>content provider</td>
<td>value of token</td>
<td>integrity</td>
<td>8</td>
</tr>
</tbody>
</table>

© Johan Peeters bvba

risk

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

© Johan Peeters bvba
### assignment 5

rank the risks

**timebox: 5 mins**

---

### format output

<table>
<thead>
<tr>
<th>adversaries</th>
<th>targets</th>
<th>value</th>
<th>damage</th>
<th>cost</th>
<th>risk</th>
<th>ranking</th>
</tr>
</thead>
<tbody>
<tr>
<td>end user</td>
<td>confidentiality</td>
<td>1</td>
<td>5</td>
<td>2</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td></td>
<td>content</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>integrity</td>
<td>1</td>
<td>5</td>
<td>13</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>account</td>
<td>integrity</td>
<td>3</td>
<td>8</td>
<td>1</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>content provider</td>
<td>value of token</td>
<td>integrity</td>
<td>8</td>
<td>8</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>
assignment 6

which risk should we
• externalize?
• absorb?
• mitigate with procedural controls?
• mitigate with technical measures?

**timebox: 10 mins**

© Johan Peeters bvba

- threat model
- risk mitigation strategies
- work items