Protection Poker: an Agile Security Risk game

Agile2014

Laurie Williams  laurie.williams@gmail.com
Catherine Louis  cll@cll-group.com

#SecDojo
Think Like a Thief

Put yourself in the mind of a thief ... **Plan a heist!**

Choose a scenario that would have a high chance of success, lay out the details ...

How long do you think it would take to plan & execute the theft? How much would you hope to gain in terms of value ($ or otherwise)? What would be the effect of the theft on the victim?
Think Like a Hacker

Put yourself in the mind of a hacker ... plan an attack on a computer system!

Choose a scenario that would have a high chance of success, lay out the details ... how long do you think it would take to plan & execute the attack? How much would you hope to gain in terms of value ($ or otherwise)? What would be the effect of the attack on the victim?
Debrief

We can only invest in a few of these thefts & attacks ... how should we choose?

Share your payoffs ... share how much time you are willing to invest

What are the characteristics ... of a hard heist? ... of an easy heist?

Why would you bother with a hard heist?
CAUGHT ON CAMERA

“SLIDERS” PREY ON WOMEN AT GAS STATIONS
STEALING PURSES IN A FLASH
### Software Security Risk Assessment

<table>
<thead>
<tr>
<th>Impact</th>
<th>Ease</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low Impact</td>
<td>Difficult to Exploit</td>
<td>Lowest</td>
</tr>
<tr>
<td>High Impact</td>
<td>Easy to Exploit</td>
<td>Highest</td>
</tr>
</tbody>
</table>
Value Points

.5 .8 .13 .20 .40 .100

High Value

Ease Points

1 .2 .3 .5 .8 .13 .20 .40

Hard to Attack

The following about the new feature are some things that would make the system harder to attack:
- New feature does not create any new pages or user input fields.
- New feature reduces the current number of pages or user input fields.
- Exceptions are all handled properly to prevent information leakage.

The following about the new feature are some things that would make the system easier to attack:
- New feature adds new pages.
- New feature adds new user input fields
- New feature has few (or one) role(s) with significant read, write, update authority.
- New feature requires a significant change in access control (permissions).
- New feature provides default usernames and passwords when the product is shipped.
- New feature does not enforce strong passwords.
Welcome Random Person!

Announcements

New features in iTrust

- Very happy or upset about your last office visit? Fill out a survey and let us know!
- You can now schedule appointments with HCPs found in Survey Results!
- No more typing in a date! We now have a calendar popup that makes scheduling appointments easier.

Notifications

Appointments in the next week

No Upcoming Appointments

Appointment Requests Needing Your Response

View your appointment history here

No Appointment Requests

Surveys that still need to be completed

- Complete survey for office visit 11
- Complete survey for office visit 1

Comprehensive Report History

- Request was requested on 01/05/2008 12:00 by Kelly Doctor
- Request was requested on 06/01/2008 12:00 by Kelly Doctor and approved on 02/06/2008 12:00
Step 1: Calibrate value points of database tables (done once)

Which database table would be least attractive to an attacker? ... most attractive?

Assign a 1 to the least attractive table.

How times more valuable is the most attractive table versus the least attractive?

These are your “value” endpoints.
Step 2: Calibrate ease points of attack for feature (done once)

Which feature adds functionality that will make an attack easiest? ... hardest?

How times easier is the easiest feature to hack versus the hardest feature?

These are your “ease” endpoints.
Some new features.

- New user role ... emergency responder (aka ambulance driver) who can get critical data
- Find qualified doctor for new diagnosis
- Update diagnosis code table
- Patients can view access log
feature

Value: Identify database tables used in that requirement. For each:

- Table already have a “value”? Use it.
- Table doesn’t have a “value”? “Poker” a value.

Ease: “Poker” a value for ease points. Discuss changes to implementation that may reduce the ease.

Compute security risk by multiplying value by ease.
Example: Security Risk Assessment

<table>
<thead>
<tr>
<th>Feature</th>
<th>Ease Points</th>
<th>Value Points</th>
<th>Security Risk</th>
<th>Rank</th>
</tr>
</thead>
<tbody>
<tr>
<td>Feature 1</td>
<td>1</td>
<td>100</td>
<td>100</td>
<td>3</td>
</tr>
<tr>
<td>Feature 2</td>
<td>5</td>
<td>1</td>
<td>5</td>
<td>6</td>
</tr>
<tr>
<td>Feature 3</td>
<td>5</td>
<td>1</td>
<td>5</td>
<td>6</td>
</tr>
<tr>
<td>Feature 4</td>
<td>20</td>
<td>5</td>
<td>100</td>
<td>3</td>
</tr>
<tr>
<td>Feature 5</td>
<td>13</td>
<td>13</td>
<td>169</td>
<td>2</td>
</tr>
<tr>
<td>Feature 6</td>
<td>1</td>
<td>40</td>
<td>40</td>
<td>5</td>
</tr>
<tr>
<td>Feature 7</td>
<td>40</td>
<td>60</td>
<td>2400</td>
<td>1</td>
</tr>
</tbody>
</table>
Step 4: Risk Ranking and Discussion

Rank your risks.

Any surprises? Satisfied with values you gave?

What plans would you put in place now that you are more aware of the security risk?
RedHat Case Study

Current software security knowledge: PP learn about software security.

Focus on true software security risks: PP help spread software security knowledge.
Discussions

(a) 
- Seth: 14%
- Manager: 14%
- Colin: 7%
- Ethan: 11%
- Owen: 7%
- Noah: 11%
- Paige: 20%
- Luke: 14%

(b) 
- Ethan: 0%
- Seth: 16%
- Manager: 28%
- Noah: 7%
- Paige: 21%
- Luke: 13%
- Owen: 8%
- Adam: 2%
Poker

Explicit result (<20%):

Relative security risk assessment

Side effects/implicit results (80%+):

Greater awareness understanding of security implications of requirement

Collaborative threat modeling & misuse case development

Requirements changed to reduce risk

Allocation of time to build security into new functionality, "delivered" at end of iteration (appropriate to relative risk)

Knowledge sharing and transfer of security information
Your Turn: Play Protection Poker!

Collaborative work on debating value and use ... subjectively, not using cards (would take too long!) [20 minutes]

Produce a ranked list of the security risk of the features ... what actions could be taken to mitigate risk [5 minutes]

ready to share!