

Tracking agile security requirements

Johan Peeters,
independent software architect

objective

Show how to integrate security requirements into an agile development project

Schedule

- 0 - 15 min: system to build
 - user stories
- 15 – 35 min: identify
 - assets
 - potential attackers
- 35 – 60 min: write abuser stories in small groups

BREAK

Schedule/2

- 60 – 85 min: plenary
 - review abuser stories
 - assessment of cost of abuser stories
- 85 - 115 min: planning game
 - Estimate effort needed to refute abuser stories
 - Schedule effort
- 115 - 135 min: evaluation

FreeSlots

Please visit our sponsors →
Your game won't be interrupted.

SLOTLAND Quick Start Menu

Choose a game:

Slots

Video Poker

Blackjack

More slots to play:
[Lucky Nugget](#)
[SuperSlots](#)

3 Scattered "Fruit Smoothie" Blenders in any position triggers the Smoothie Bonus



Paytable

WIN	PAID	CREDITS	BET
		75	7

On

CASH CREDIT

PLAY 1 LINE

PLAY 3 LINES

PLAY 5 LINES

PLAY 7 LINES

PLAY 9 LINES

SPIN REELS

A user story: gamble

The user presses the start button and the reels start spinning. If a payline shows a winning combination, credit is incremented according to the pay table.

Another user story: logging in

A user authenticates. The system retrieves his details. In particular, his credit becomes available.

An abuser story: increase credit

A wily hacker increases his credit without paying.



Picture from Cigital press release

This screenshot shows the software interface for the poker game. On the right, the 'Game Parameters' window is open, showing:

- Num Players: 3
- Your Position: 1
- Your Cards: 8c, Jh
- Flop: Js, 9c, 2d

 A 'Show Cards' button is located below these parameters. In the center, the flop cards are shown again: J♠, 9♣, 2♦, 4♠, and 7♣. On the left, there are input fields for 'Minute Offset' (-1) and 'Second Offset' (52), a 'Shuffle Button', and a 'Time' display (16:21:40). At the bottom, there are buttons for 'FOLD' for each of the three players, followed by their respective card counts (3, 1, 2). Below these are the cards for each player:

- Player 3: 8♦, 4♦
- Player 2: 7♥, 9♠
- YOU: J♠, 8♣

Picture from Cigital paper 'How we Learned to Cheat in Online Poker'

Another abuser story: predict outcome

A wily hacker is able to predict the symbols on the payline and hence stakes little when they will not amount to a winning combination and lots when they will.

Anatomy of an abuser story

A **wily hacker** is able to predict **the symbols on the payline** and hence stakes little when they will not amount to a winning combination and lots when they will.

Attacker
risk?

Asset
impact?

Another anatomy

A wily hacker increases his credit without paying.

Attacker

skill: high

motivation: 'because I can'

time: immaterial

resources: low

Asset

direct effect on revenue

planning

What is the business value of the user story?

What is the cost of the abuser story?

cost = risk x impact

How much effort does it take to implement the user story?

How much effort does it take to construct a refutation for the abuser story?

Iteration plan

- How much effort can we expend in 1 iteration?
- Maximize business value delivered in the next iteration?
 - total value = \sum value user story - \sum cost abuser story
 - total effort = \sum effort = given