

Security Personas

Making security testing personal

Laura Bell

FOUNDER & LEAD CONSULTANT
SAFESTACK

@lady_nerd

laura@safestack.io

Security Persona

Security personas identify the user motivations, expectations and goals responsible for driving **bad behaviour**, and bring users to life.

Key Concept

Three elements of security personas

Motivation

What drives this individual or group to act

Resources

Access to essentials including money, expertise and access

Skill

Ability to achieve their objective

Motivations



Motivations give clues to attacker objectives



Steal money

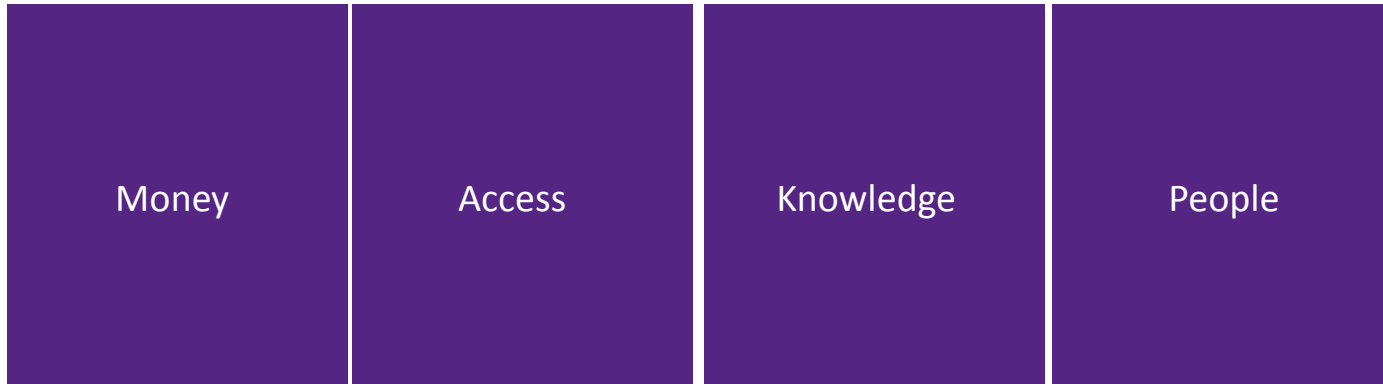
Steal things to sell for money

Corporate espionage

Extortion

Insider trading

Resources affect the details of the attack



Resources can directly affect success

Speed and Length

How long would the attack take to plan and execute?

How long it can be sustained?

Sophistication

How complex is the attack?

How easy it is to detect?

Likelihood

What is the chance that the attack will be carried out?

What is the chance that it will be successful?

Skill level

Amateur

- Enthusiastic but often slow / error prone
- Heavily reliant on learning resources
- May be easy to detect

Expert

- Experienced and knowledgeable for their domain
- Unlikely to consult outside sources
- May be difficult to detect

Attack Plans

Once you know why someone would do bad things
It's time to figure out how they would do it

Key Concept

Our first security persona



Name

Narrative

Motivation and objectives

Skill Level

Resources

Attack plan

SECURITY PERSONA:	ATTACK PLAN	
NARRATIVE		
<p data-bbox="428 199 805 264">Who?</p>		<p data-bbox="1265 347 1449 511">How? When? Where? Outcome?</p>
MOTIVATION AND OBJECTIVES		
<p data-bbox="428 521 805 586">Why?</p>		
RESOURCES	SKILL	
<p data-bbox="428 918 805 982">Using?</p>		

SECURITY PERSONA: Brian Bobson	ATTACK PLAN	
<p>NARRATIVE</p>	<p>Attack 1</p>	
<p>Brian Bobson is a 27 year old receptionist. He was employed by \$org for 4 years until he was made redundant last year. Since leaving \$org he has struggled to find a new job.</p>	<p>Physical theft from premises</p> <ul style="list-style-type: none"> • Computer equipment • Mobile devices <p>Sale of items to local fence or online market places</p>	
<p>MOTIVATION AND OBJECTIVES</p>	<p>Attack 2</p>	
<ul style="list-style-type: none"> • Frustrated and angry at loss of long term job • Financial difficulty from loss of employment 	<p>Data theft from premises</p> <ul style="list-style-type: none"> • Documents • Removable media • Laptops <p>Sale to competitors of \$org or use for extortion.</p>	
<p>RESOURCES</p>	<p>SKILL</p>	
<ul style="list-style-type: none"> • Low funds • Large amount of free time • Well liked amongst current and former employees • Previous access details such as door and alarm codes. 	<ul style="list-style-type: none"> • Low technical skill 	

Uses for security personas



Security depends on collaboration

- Share your security personas
 - Apply them to projects
 - Apply them to the overall organisation
- Make a central wall or board to display your 'most wanted'
 - Create a culture of security discussion
 - Make security personas an interactive part of the office

Summary

- Develop security personas for your application
- Consider the motivation, resources and skill level for each persona you develop
- Include your persona in requirements capture to identify security mitigations
- Security personas can be used to guide in house security testing
- Make your security personas available to all teams within your organization – get everyone involved.

Questions?

Laura Bell

FOUNDER & LEAD CONSULTANT
SAFESTACK

@lady_nerd

laura@safestack.io