

# Threat Personas and Application Vulnerability Scoring Model

Phil Huggins & Robin Oldham  
CISO Mentor & Cydea



# Objectives of this session

1. Borrow UX concept of personas for a structured and reusable way to consider and discuss threats
2. Create some *Threat Personas*!
3. Explore a fast, developer-friendly way to use them and prioritise vulnerabilities



**Phil Huggins**

[@oracuk](#) / [LinkedIn](#)

CISO Mentor



**Robin Oldham**

[@RTO](#) / [LinkedIn](#)

Cydea



[Follow along / ask questions on Twitter](#)

## Looking for outputs?

Check these GitHub repos:

- [Threat Personas](#)
- [VSort](#)



CISO Mentor

cydea



# AUDIENCE PARTICIPATION AHEAD



# The plan...

- 11:00 Introduction to *threat personas*
- 11:15 Break out - create some!
  - 15m Groups of ~5, create your persona
  - 5m Crowd-sourced some attributes
  - 15m Present back
- 11:50 Short break
- 12:00 Introduction to app vulnerability scoring
- 12:20 Worked example
- 12:30 Your turn (based on your group/persona)
- 12:45 Questions




# Threat Personas



# What are user personas?

Name and biographical info  
help reader connect with them

Other useful metadata



**NAME:**  
Sandeep

**AGE:**  
28

**FROM:**  
Maharashtra, India

**LIVES:**  
Delhi, India

**OCCUPATION:**  
Research Scholar

**BIOGRAPHY**

Sandeep is a PhD student at Jawaharlal Nehru University (JNU), a leading liberal arts university located in Delhi. He has always been dedicated to his studies because he believes in the value of a good education. He enjoys spending time with his professors and even thinks of them as friends.

Sandeep was introduced to computers in secondary school. He attended one of the most reputable English-medium private schools in his state, one for the children of military parents. There, he learned to type, conduct online research, and create high-quality reports and presentations.

His parents gave Sandeep a feature phone when he moved to Delhi to pursue a Bachelor's in History, because his mother wanted a means to stay in touch with him. After graduation, he enrolled in a Master's at JNU, and his friends convinced him to buy a smartphone so they could communicate on WhatsApp. Sandeep was initially hesitant to spend his meager JNU research stipend (Rs 1,000 or \$45 a month), but agreed to buy it after one of his professors hired him for a research project. His friends recommended he buy an LeEco Le 1s Android phone (Rs 12,000 or \$180) because it was a good value.

When on campus, Sandeep uses JNU's WiFi—he even has a private WiFi connection in his hostel room. When he's off campus, he has a data plan to access the internet on his phone. He uses a Dell laptop for research, writing, and studying for exams. He relies on his professors for academic information, but also supplements what they provide through Google searches and reliable sources (including JSTOR.org and EPW.in, Economic and Political Weekly) recommended by his professors and peers.

For any research project, Sandeep begins by searching on Google. He typically starts with relatively broad search terms and, based on the results they yield, will make his queries more targeted over time. During his Master's program, he learned what types of sources can be trusted. As a result, he will only use Wikipedia for topic overviews and as a source for references.

Sandeep's English is at near-native proficiency; as a result, he usually has no problem finding what he needs online. He uses a translation app for esoteric and unfamiliar English words that are few and far between. The only time he remembers searching in a language other than English was while doing a project on a local political movement in rural Maharashtra.

**DEVICE USE**

**LeEco Le 1s Android smartphone**


**PRIMARY USE:** Voice calls, WhatsApp, following conversations between friends but rarely participates himself.

**NETWORK:** Internet usage is mostly via WiFi on university campus because it is free. Platform data on his phone is gone out. He pays Rs 288 a month for his plan.

**Personal Dell laptop**


**PRIMARY USE:** Uses it for research, writing papers, etc.

**DETAILS:** Goes online in his hostel, and carries it to campus where he accesses the university's internet.



**Low Digital Confidence** ————— **High Digital Confidence**

**Low Economic Status** ————— **High Economic Status**



**NAME:**  
Helen

**AGE:**  
35

**FROM:**  
Anambra, Nigeria

**LIVES:**  
Epe, Nigeria

**OCCUPATION:**  
Tailor

**BIOGRAPHY**

Helen lives in a small town, Epe, with her husband, a laborer at the nearby noodle factory, and their three young children. Although her family struggles to make ends meet, Helen is very economically resourceful. After giving birth to her first child to years ago, she became a seamstress to supplement her family's income.

Helen keeps track of local happenings by chatting with neighbors or listening to her husband and his friends when they come to chat in the evenings. She's most interested in news that impacts her and her family: gossip about teachers at her children's school, rumors of possible protests or strikes, and other community news.

Helen uses a low-grade smartphone mostly for calls and some web browsing. Her internet access is limited by the frequent power cuts—her family doesn't own a generator—and her ability to pay for data. To get online she relies almost exclusively on the free data that comes as a bonus with airline purchases. Helen switches on her data only when necessary. She's frustrated that the connection is often unreliable—even the rate seems to affect it. When she is online, her top priority is staying connected with family and friends. Facebook is her favorite app, which she joined at the urging of a cousin who studies abroad. This was also the beginning of her internet usage.

Since then, she has found many other uses for the internet: she looks up confusing phrases from the Bible, searches for ideas to grow her business, and gets outfit inspiration before big social events. She is amazed at the seemingly never-ending amount of information "Mr. Google," her favorite search engine, can provide.

Helen recognizes the Wikipedia icon on her mobile phone but doesn't know what it is—she thinks it may have come with her phone. She has opened the app before out of curiosity but was uncertain of what she should do and quickly closed it.

**DEVICE USE**

**Infinix Android Race Eagle X50 Smartphone**

**PRIMARY USE:** Voice calling, Facebook, and internet browsing.


**NETWORK:** Airtel. Tops up N500 to N200 (\$0.35 to \$0.70) every week or two, which gets her data bonus of 50 to 20 MB. This is her primary line.

**APPS USED:** In order of preference: Facebook, WhatsApp.

**Tecno T410 (dual sim)**

**PRIMARY USE:** Voice calling.

**NETWORK:** Glo & Enatel, as it is difficult to depend on one network given patchy connectivity. Uses both as backup when the Airtel network is down, so doesn't always have credit on them. Tops up N50 (\$0.35) at a time, as needed.



**Low Digital Confidence** ————— **High Digital Confidence**

**Low Economic Status** ————— **High Economic Status**

More detailed narrative  
about them and what makes  
them tick

Characteristics or  
attributes. What  
they care about



CISO Mentor

cydea

RE3BOOT

RE3BOOT

# Threat Personas

A **threat persona** is a narrative describing a fictional individual that embodies the characteristics of the threat actor under consideration.

This allows us to **structure** our consideration of threat actors in a **reusable** and **calculable** way.

The *Threat Actor Library* (TAL) developed by Tim Casey is a good example of this approach (though a bit 'GRC' in its use of language.)

Here we use some more developer-friendly language to do the same thing.

**Generate these in advance** for your organisation and use to inform developers about the threat they face during threat modelling sessions and application risk assessments.

## Characteristics:

- **Internal/External**
- **Malicious/Non-Malicious**
- **Goals** (Curiosity, Personal Fame, Personal Gain, National Interests, Revenge, etc)
- **Skills** (No technical skills, End user, Power user, Developer, Researcher)
- **Knowledge** (External to organisation, Ex-Organisation insider, Organisation partner, Customer, Employee, Other insider)
- **Opportunity** (Connected to Internet, Physically nearby, Access to connected partner, Access to organisation, Access to specific network / system)
- **Deterrability** (Unconcerned criminal, Careful criminal, Careless law-abiding, Careful law-abiding)



# Disgruntled Customer

**Summary:** Marie Bourdin is a customer of the business. She has consistently pushed to get access to drugs that our doctors have been uncomfortable prescribing to her. She is becoming frustrated with the business and is continuing to press for access to drugs but is starting to think about revenge. ([External](#), [Malicious](#))

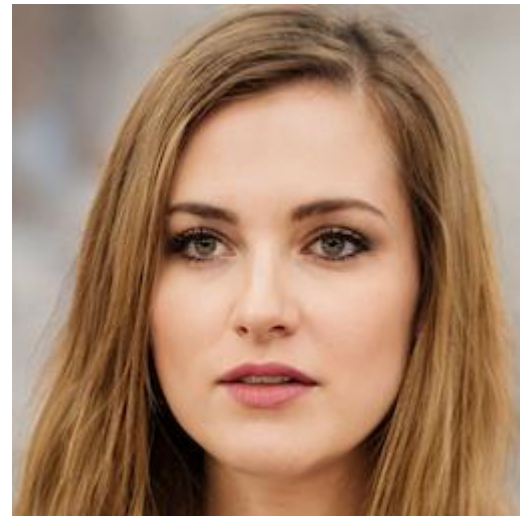
**Goals:** Her main goal is to gain access to drugs that the doctors are not comfortable prescribing to her. Her secondary goal is to disrupt the business when we refuse to provide access to the drugs. ([Personal Gain](#), [Revenge](#))

**Skills:** Marie is no technical expert but she is clever and capable of understanding how systems work. ([Power User](#))

**Knowledge:** She is building up knowledge of how the business works every time she interacts with us. ([Customer](#))

**Opportunity:** Marie has no special access to the business other than via the Internet. ([Connected to the Internet](#))

**Deterrability:** Marie is prepared to break the law to achieve her goals but is methodical and careful in her approach. ([Careful Criminal](#)).





# Disgruntled Insider

**Summary:** Dr Chiara Romano is a member of the clinical team. She has been growing increasingly frustrated as she perceives she is being unfairly denied a promotion. She doesn't intend to commit criminal acts but as her frustration becomes anger she becomes focused on expressing her anger and may not realise how far she is going. ([Internal / Malicious](#))

**Goals:** Her goal is to cause disruption and distress to the management team although she does not want to cause any physical harm to a patient. ([Revenge](#))

**Skills:** She is a typical end-user with little deeper understanding and no access to exploits or knowledge of how to conduct scripted attacks. ([User](#))

**Knowledge:** Chiara knows how the organisation works and knows the systems she uses for her day to day job. ([Organisation Employee](#))

**Opportunity:** She has access to the building as does any employee but also has access to SYSTEM A as a doctor. ([Access to Organisation](#))

**Deterrability:** Chiara doesn't believe she is criminal, she believes she is right but still acts in order to avoid detection. ([Careful Criminal](#)).



# Misha Melnyk: Career criminal



## EXTERNAL, MALICIOUS

Misha Melnyk is a career criminal who believes himself out of the reach of the authorities although he is careful not to commit crimes in his home country. He has been an active criminal online for about 10 years. He regularly buys exploits on the dark market but is not himself a developer.

## GOALS

Personal Gain

## OPPORTUNITY

Connected to the Internet

## SKILLS

Power User

## KNOWLEDGE

External to organisation

## DETERRABILITY

Unconcerned criminal



Your turn!  
-->

Open this 

[OSS2020 Threat Personas](#)

(link also in chat)



# (Breakout Rooms working on Threat Personas)



(Quick present back Persona output)



Next up --> Blitz this form 

## Threat Persona Characteristics

(link also in chat)



(\*Phew\* short break... Start back 12:00!)



# Application Vulnerability Scoring





# Scoring Model Goals

Simple and explainable

Short, no more than 10 questions

Developer-friendly language

Question & answer driven

*Relative* prioritisation not objective risk



# 10 Questions

1. How skilled is the attacker?
2. Do the attackers have the knowledge they need to attack?
3. Why would the attacker attack us?
4. Will they work within legal and ethical boundaries?
5. How likely are they to find us?
6. How hard is the vulnerability to find?
7. How hard is the vulnerability to use?
8. How many authentication steps are required to attack the vulnerability?
9. Is the vulnerability protected from attack?
10. Is the system monitored for attacks on the vulnerability?



# 10 Model Parameters

## Attacker

1. Attacker Skill
2. Attacker Knowledge
3. Attacker Reward
4. Attacker Deterrability
5. Attacker Recon Approach



(Get these from the appropriate Threat Persona)

## Vulnerability

6. Vuln Findability
7. Vuln Exploitability
8. Vuln Authentication
9. Vuln Protection
10. Vuln Monitoring



# Model Components

## Skill:

(Attacker Skill **vs** Vuln Exploitability) **and** (Attacker Skill **vs** Vuln Authentication)

## Opportunity:

(Recon Approach **and** Attacker Skill **and** Attacker Deterrability) **vs** Vuln Findability

## Motivation:

Attacker Reward **and** Skill **and** Opportunity

## Success:

Motivation **vs** (Vuln Protection **and** Vuln Monitoring)



# Spreadsheet Implementation

Threats	How skilled is the attacker?	Score	Do the attackers have the knowledge they need to attack this vulnerability?	Score	Why would the attackers attack this vulnerability?	Score	How likely are they to find this vulnerability?	Score	How likely are they to break Legal or Ethical boundaries ?	Score
	Security Researcher	10	Public Knowledge	10	High Reward	10	Internal User	10	Will break legal and ethical boundaries	4
	Developer	8	Cursory Inspection	8	Some Reward	6	Mass Scanning	8	on the limits of what is legal	1
	Power User (Scripting)	4	Private Knowledge	4	Minimal Reward	4	Accident	6	Works within Legal and ethical boundaries	-2
	User (Basic Literacy)	1	Confidential Knowledge	1	No Obvious Reward	2	Targeted	2		
Vulnerability	How hard is the vulnerability to find?	Score	How hard is the vulnerability to use?	Score	How many authentication steps are required to use the vulnerability?	Score	How well do we protect the vulnerability from attack?	Score	Are we watching for the vulnerability to be used?	Score
	Automated	1	Automated	1	None	0	None	0	No	0
	Easy Manual	2	Easy Manual	2	One	4	Ineffective Control	2	Performance Monitoring	4
	Skilled Manual	6	Skilled Manual	6	Two	6	Hide the vuln	4	Security Monitoring	6
	Hard Manual	8	Hard Manual	8	More than Two	10	General Control	6	Exploit-Specific Monitoring	10
	Almost Impossible	10	Almost Impossible	10			Vulnerability-Specific Control	10		

Attacker Skill	(How Skilled - How Hard) - (How Skilled - Number of Auths)
Attacker Opportunity	(Likely to Attack + How Skilled + Ethical/Legal boundaries) - How hard to Find
Attacker Motivation	(Why attack + Attacker Skill + Attacker Opportunity)
Likelihood of Attacker Success	Attacker Motivation - (How well protected + How well Monitored)



# Worked Example

## Attacker

### Disgruntled Insider

OPEN  
SECURITY SUMMIT

**Summary:** Dr Chiara Romano is a member of the clinical team. She has been growing increasingly frustrated as she perceives she is being unfairly denied a promotion. She doesn't intend to commit criminal acts but as her frustration becomes anger she becomes focused on expressing her anger and may not realise how far she is going. (Internal / Malicious)

**Goals:** Her goal is to cause disruption and distress to the management team although she does not want to cause any physical harm to a patient. (Revenge)

**Skills:** She is a typical end-user with little deeper understanding and no access to exploits or knowledge of how to conduct scripted attacks. (User)

**Knowledge:** Chiara knows how the organisation works and knows the systems she uses for her day to day job. (Organisation Employee)

**Opportunity:** She has access to the building as does any employee but also has access to SYSTEM A as a doctor. (Access to Organisation)

**Deterrability:** Chiara doesn't believe she is criminal, she believes she is right but still acts in order to avoid detection. (Careful Criminal).



1. Attacker Skill
2. Attacker Knowledge
3. Attacker Reward
4. Attacker Deterrability
5. Attacker Recon Approach

- = User (1)
- = Private Knowledge (4)
- = Some Reward (6)
- = Will break Ethical & Legal boundaries (4)
- = Internal User (10)



CISO Mentor

cydea

# Worked Example

## Vulnerability

Broken access control allows an internal user to enumerate records owned by a different internal user by incrementing record identifier in the URL.

6. Vuln Findability	= Automated (1)
7. Vuln Exploitability	= Automated (1)
8. Vuln Authentication	= None (0)
9. Vuln Protection	= None (0)
10. Vuln Monitoring	= Security Monitoring (6)



# Worked Example

## Calculation

$$\begin{aligned}\text{Attacker Skill} &= (1-1)-(1-0) &= -1 \\ \text{Atatcker Opportunity} &= (10 + 1 + 4) - 1 &= 14 \\ \text{Attacker Motivation} &= (6 + -1 + 14) &= 19 \\ \text{Atatcker Success} &= 19 - (0 + 6) &= 13\end{aligned}$$

**Broken Access Control Vuln Score: 13**





 AUDIENCE PARTICIPATION AHEAD 



# Your turn...

We have discovered an **XSS Injection attack** via the message system on our customer web application that is available to all logged-in customer accounts.

By sending a crafted message to our customer service team via the site messaging functionality the XSS code executes in the customer service agent's browser.

The customer service agents can authorise returns, refunds and issuing gift cards as well as accessing and updating customer account data.

We do not have specific application security monitoring in the application but we do have a cloud-based WAF using the OWASP Modsecurity Core rules.



# Questions to the room

1. Are the questions developer friendly?
2. Are these the right model parameters?
3. Do the model relationships make sense?
4. Are the weightings correct?
5. What would you add or take away?



# Thank You

Robin & Phil

