OPEN SECURITY SUMMIT

June | 2020

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

🗣️ Follow along / ask questions on Twitter

Phil Huggins
@oracuk / LinkedIn
CISO Mentor

Robin Oldham
@RTO / LinkedIn
Cydea

CISO Mentor cydea

🚨 AUDIENCE PARTICIPATION AHEAD 🚨

The plan...

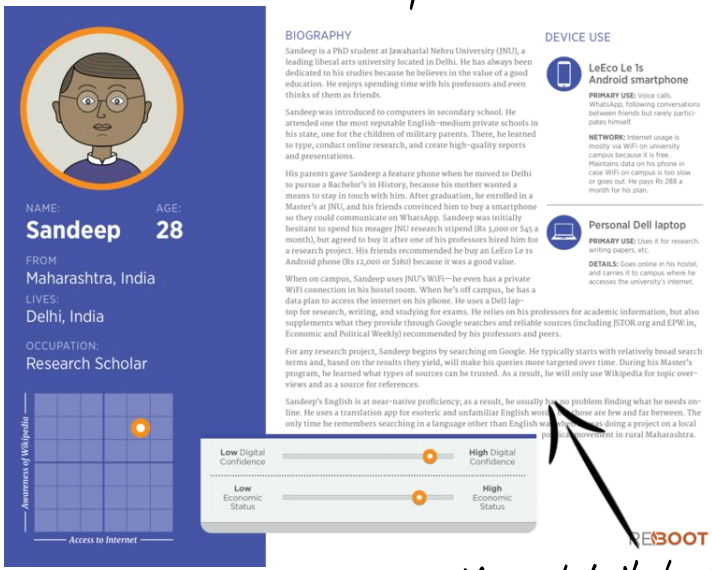
11:00	Introduction to *threat personas*
11:15	Break out - create some!
	15m Groups of ~5, create your persona
	5m Crowd-sourced some attributes
	15m Present back
11:50	Short break
12:00	Introduction to app vulnerability scoring
12:20	Worked example
12:30	Your turn (based on your group/persona)
12:45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

CISO Mentor cydea

Threat Personas

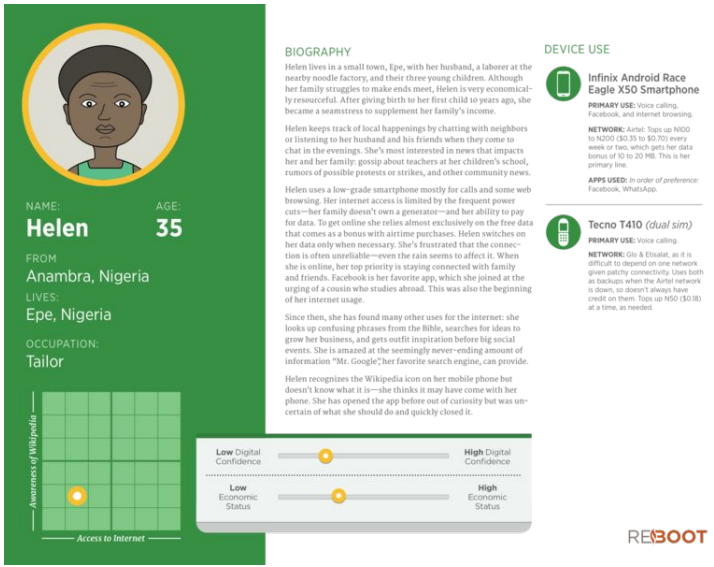
What are user personas?

Name and biographical info
help reader connect with them



More detailed narrative
about them and what makes
them tick

Other useful metadata



Characteristics or
attributes. What
they care about

CISO Mentor cydea

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)

Derived from Open Information Security Risk Universe: www.oisru.org and the Intel TAL.

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)

Deterrabilty: Marie is prepared to break the law to achieve her goals but is methodical and careful in her approach. (Careful Criminal).

External Criminal

Summary: 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. (External, Malicious)

Goals: Wants to make money. Misha's goal is to obtain payment data, medical data, personal data and system access which he then sells on the dark market for profit. (Personal Gain)

Skills: He is technical enough to read a manual and use scripted attacks and exploits but he does not develop custom attacks. If the tools he has fail then he moves on to other targets. (Power User)

Knowledge: May have access to specific technical knowledge about platforms or tools used by the business but unlikely to have specific knowledge either of our business processes or code. (External to Organisation)

Opportunity: Has unfettered access to the public Internet but no more than that. (Connected to Internet)

Deterrabilty: He will conduct criminal acts on the Internet without constraint. (Unconcerned Criminal)

CISO Mentor cydea

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)

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

Security Researcher

Summary: David ‘Z3r0’ Smith is a security researcher who works a day job as a penetration tester and participates in bug bounties in his spare time to earn more money. He has only three years experience in the role. He is not well known on the hacking scene and is using public vulnerability disclosures and capture the flag contests to build his profile. (External / Non-Malicious)

Goals: Wants to build a public reputation for security research in order to progress career and achieve personal recognition. May also be looking for ‘bug bounty’ money. (Curiosity / Personal Fame)

Skills: Highly technically skilled with specific security skills. Likely also to have access to a network of highly technically skilled individuals. (Researcher)

Knowledge: May have access to specific technical knowledge about platforms or tools used by the organisation but unlikely to have specific knowledge either of the organisation’s business processes or code. (External to Organisation)

Opportunity: Has unfettered access to the public Internet but no more than that. (Connected to Internet)

Deterrability: Will not try to commit criminal acts but may through ignorance or arrogance ‘go too far’ without malicious intent. (Careless law-abiding).

OPEN SECURITY SUMMIT

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)

CISO Mentor cydea

OPEN SECURITY SUMMIT

(Breakout Rooms woking on Threat Personas)

CISO Mentor cydea

(Quick present back Persona output)

Next up--> Blitz this form 👇

[Threat Persona Characteristics]

(link also in chat)

CISO Mentor cydea

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

OPEN SECURITY SUMMIT

Application Vulnerability Scoring

CISO Mentor cydea

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)

CISO Mentor cydea

Worked Example

Attacker

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)

Deterrabilty: 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 = User (1)
2. Attacker Knowledge = Private Knowledge (4)
3. Attacker Reward = Some Reward (6)
4. Attacker Deterrability = Will break Ethical & Legal boundares (4)
5. Attacker Recon Approach = 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

Attacker Skill	= (1-1)-(1-0)	= -1
Atatcker Opportunity	= (10 + 1 + 4) -1	= 14
Attacker Motivation	= (6 + -1 + 14)	= 19
Atatcker Success	= 19 - (0 + 6)	= 13

Broken Access Control Vuln Score: 13

CISO Mentor cydea

🚨 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?

OPEN SECURITY SUMMIT

Thank You

Robin & Phil

CISO Mentor cydea