



Adaptive Authentication in Keycloak

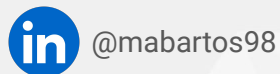
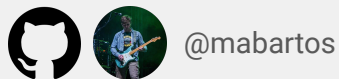
Authentication Policies, Risk-based Authentication and AI



\$ whoami

Martin Bartoš

Senior Software Engineer



Context

Context

- Topic of my master's thesis

Context

- Topic of my master's thesis
- The goal was to provide **PoC** of integrating **Adaptive Authentication**

Context

- Topic of my master's thesis
- The goal was to provide **PoC** of integrating **Adaptive Authentication**
- **Keycloak Extension** (github.com/mabartos/keycloak-adaptive-authn)

Context

- Topic of my master's thesis
- The goal was to provide **PoC** of integrating **Adaptive Authentication**
- **Keycloak Extension** (github.com/mabartos/keycloak-adaptive-authn)
- Trying to touch the Keycloak codebase as little as possible

What is Adaptive Authentication ?

Adaptive Authentication

- **Dynamic** user identity verification mechanism

Adaptive Authentication

- **Dynamic** user identity verification mechanism
- Change authentication requirements in **real-time**

Adaptive Authentication

- **Dynamic** user identity verification mechanism
- Change authentication requirements in **real-time**
- Mostly rely on **Risk-based** authentication

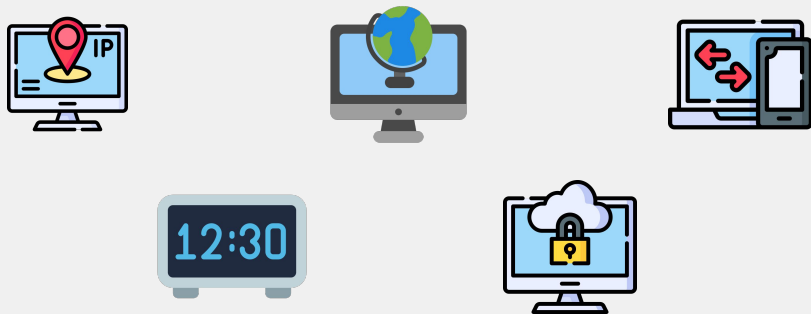
Adaptive Authentication

- **Dynamic** user identity verification mechanism
- Change authentication requirements in **real-time**
- Mostly rely on **Risk-based** authentication
- Use **multiple context** information



Adaptive Authentication

- **Dynamic** user identity verification mechanism
- Change authentication requirements in **real-time**
- Mostly rely on **Risk-based** authentication
- Use **multiple context** information



Multi-Factor Authentication

Static

Brief

Definite
beginning
and end

Adaptive Authentication

Flexible

Ongoing

Never
ends

Figure 1. MFA vs Adaptive Authentication

Pros & Cons

Pros & Cons

+ **Strengthen security**

additional factors required when accessing sensitive resources

Pros & Cons

- + **Strengthen security**
- + **Better UX**

additional factors required when accessing sensitive resources
do **not require factors** when not necessary

Pros & Cons

+ **Strengthen security**

+ **Better UX**

+ **Context-aware protection**

additional factors required when accessing sensitive resources

do **not require factors** when not necessary

more information about the authentication attempt

Pros & Cons

- + **Strengthen security**
- + **Better UX**
- + **Context-aware protection**
- + **Flexibility**

additional factors required when accessing sensitive resources

do **not require factors** when not necessary

more information about the authentication attempt

more capabilities to meet customers' needs

Pros & Cons

- + **Strengthen security**
- + **Better UX**
- + **Context-aware protection**
- + **Flexibility**
- + **AI/ML integration**

additional factors required when accessing sensitive resources
do **not require factors** when not necessary
more information about the authentication attempt
more capabilities to meet customers' needs
provides **more knowledgeable decisions** based on AI/ML

Pros & Cons

- + **Strengthen security**
- + **Better UX**
- + **Context-aware protection**
- + **Flexibility**
- + **AI/ML integration**
- + **Simpler regulations fulfillment (DORA, NIS2)**

additional factors required when accessing sensitive resources
do **not require factors** when not necessary
more information about the authentication attempt
more capabilities to meet customers' needs
provides **more knowledgeable decisions** based on AI/ML
processing and analyzing events, **risk assessments**

Pros & Cons

- + **Strengthen security**
- + **Better UX**
- + **Context-aware protection**
- + **Flexibility**
- + **AI/ML integration**
- + **Simpler regulations fulfillment (DORA, NIS2)**

- **Initial complexity**

additional factors required when accessing sensitive resources
do **not require factors** when not necessary

more information about the authentication attempt

more capabilities to meet customers' needs

provides **more knowledgeable decisions** based on AI/ML
processing and analyzing events, **risk assessments**

implementation requires **new concepts/components**

Pros & Cons

- + **Strengthen security**
- + **Better UX**
- + **Context-aware protection**
- + **Flexibility**
- + **AI/ML integration**
- + **Simpler regulations fulfillment (DORA, NIS2)**

- **Initial complexity**
- **Risk assessment accuracy**

additional factors required when accessing sensitive resources
do **not require factors** when not necessary

more information about the authentication attempt

more capabilities to meet customers' needs

provides **more knowledgeable decisions** based on AI/ML
processing and analyzing events, **risk assessments**

implementation requires **new concepts/components**

assessment mechanism needs to be **reasonably tailored**

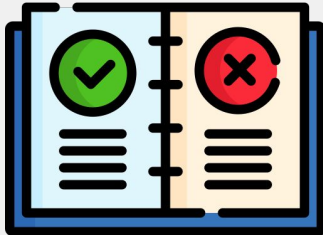
Adaptive Authentication

Parts integrated into Keycloak:

Adaptive Authentication

Parts integrated into Keycloak:

1.
**Authentication
Policies**

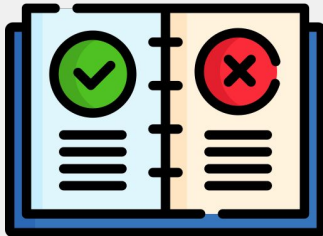


Adaptive Authentication

Parts integrated into Keycloak:

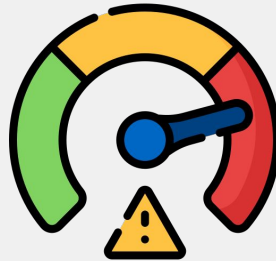
1.

**Authentication
Policies**



2.

**Risk-based
Authentication**

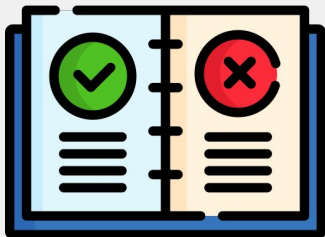


Adaptive Authentication

Parts integrated into Keycloak:

1.

**Authentication
Policies**



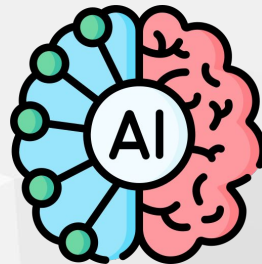
2.

**Risk-based
Authentication**



3.

**AI/ML
Approach**



Authentication Policies

Authentication Policies

- Verify that users **met specific requirements**

Authentication Policies

- Verify that users **met specific requirements**
- Define actions users **need to perform** during authentication

Authentication Policies

- Verify that users **met specific requirements**
- Define actions users **need to perform** during authentication
- Rules with **condition** → **action** syntax

Authentication Policies

- Verify that users **met specific requirements**
- Define actions users **need to perform** during authentication
- Rules with **condition** → **action** syntax
- Filter users that are able to authenticate

Authentication Policies

- Verify that users **met specific requirements**
- Define actions users **need to perform** during authentication
- Rules with **condition** → **action** syntax
- Filter users that are able to authenticate

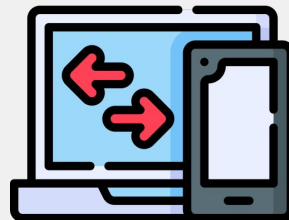
IP restrictions



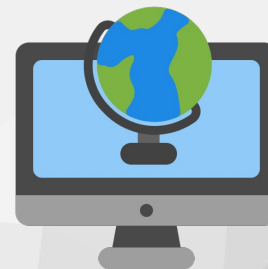
Network



Device attributes



Location



Authentication Policies

Keycloak PoC

Authentication Policies - **Keycloak PoC**

- Restricted **conditional flows**

Authentication Policies - **Keycloak PoC**

- Restricted **conditional flows**
- Separate management with the **default settings** (Admin console, REST API,...)

Authentication Policies - **Keycloak PoC**

- Restricted **conditional flows**
- Separate management with the **default settings** (Admin console, REST API,...)
- **Comprehensive rules**

Authentication Policies - **Keycloak PoC**

- Restricted **conditional flows**
- Separate management with the **default settings** (Admin console, REST API,...)
- **Comprehensive rules**
- Change **evaluation order** (priorities)









Authentication Policies - **Keycloak PoC**

- Restricted **conditional flows**
- Separate management with the **default settings** (Admin console, REST API,...)
- **Comprehensive rules**
- Change **evaluation order** (priorities)
- **Different evaluation phases** when user is not needed

Authentication Policies - **Keycloak PoC**

- Restricted **conditional flows**
- Separate management with the **default settings** (Admin console, REST API,...)
- **Comprehensive rules**
- Change **evaluation order** (priorities)
- **Different evaluation phases** when user is not needed
- **New conditions** reflecting various contexts (location, IP, device,...)

Authentication Policies - Keycloak PoC














		Flows	Required actions	Policies	Authentication policies	Risk-based policies
Steps		Enabled		Requires user		
	POLICY - Browsers Policy for handling browsers rules	<input checked="" type="checkbox"/> On		<input type="checkbox"/> No	Details	
	POLICY - Device Policy for device rules	<input checked="" type="checkbox"/> On		<input type="checkbox"/> No	Details	
	POLICY - Risk-based Policy for evaluating risk scores	<input checked="" type="checkbox"/> On		<input checked="" type="checkbox"/> Yes	Details	
	POLICY - Organizations Policy for handling organizations rules	<input checked="" type="checkbox"/> On		<input checked="" type="checkbox"/> Yes	Details	

Authentication Policies - Keycloak PoC - detail

Authentication > Authentication policy details

POLICY - Browsers

  [Add step](#) [Add condition](#) [Add policy](#)

Steps	Enabled	
  No Firefox	<input checked="" type="checkbox"/> On	    
 Condition - Browser Is Firefox	<input checked="" type="checkbox"/> On	 
 Deny access Firefox is not allowed	<input checked="" type="checkbox"/> On	 

How is it integrated into flows?

Authentication policies **Authenticator !!**

Authentication policies **Authenticator**

- Created authenticator which **separately processes different flows**

Authentication policies **Authenticator**

- Created authenticator which **separately processes different flows**
- **Separate** authentication flow **lifecycle**
















Authentication policies **Authenticator**

- Created authenticator which **separately processes different flows**
- **Separate** authentication flow **lifecycle**
- Prerequisite for ability to **reference flows in different flows**

Authentication policies **Authenticator**

- Created authenticator which **separately processes different flows**
 - **Separate** authentication flow **lifecycle**
 - Prerequisite for ability to **reference flows in different flows**
-
- *Needs to be polished*
 - *Need to resolve challenge responses*

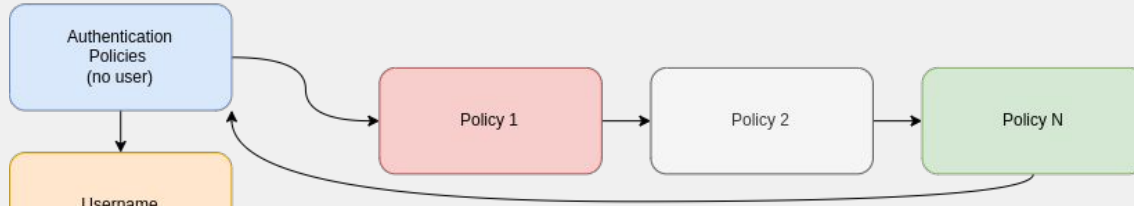
Authenticator - Simple flow

Steps	Requirement
 Authentication policies No User	Required   
 Username Form	Required  
 Password Form	Required   
 Authentication policies Requires User	Required   

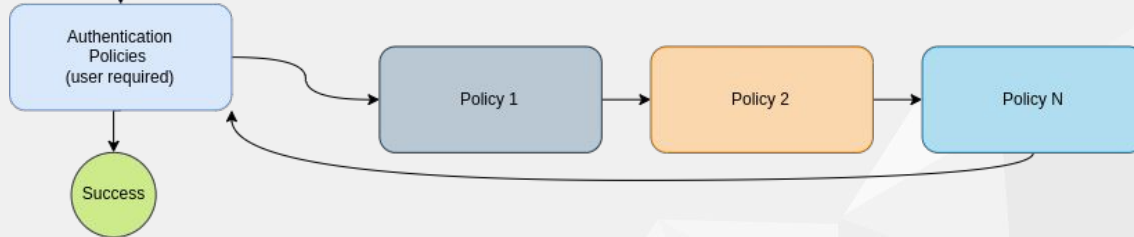
Authenticator - Simple flow

Browser Flow

Authentication Policies
Flow (no user)



Authentication Policies
Flow (user required)



Success

Risk-based Authentication

Risk-based authentication

- **Evaluate risk** (probability) **the user is imposter** - not who claims to be

Risk-based authentication

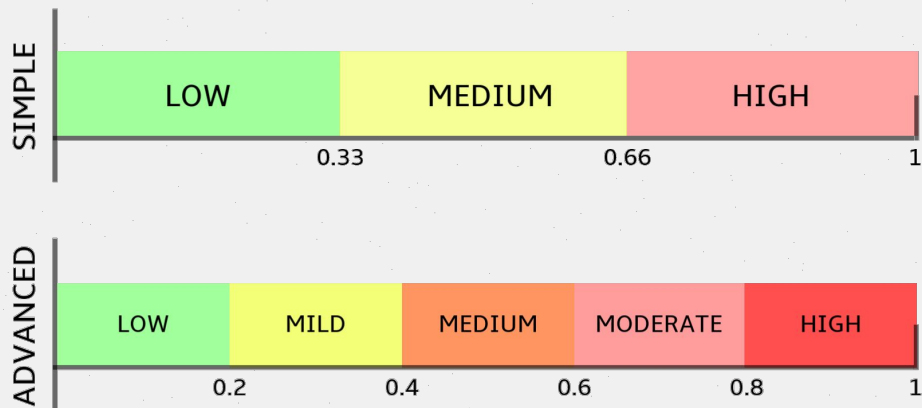
- **Evaluate risk** (probability) **the user is imposter** - not who claims to be
- Consider **multiple contexts** (IP, location, login events, browser, behavior, ...)

Risk-based authentication

- **Evaluate risk** (probability) **the user is imposter** - not who claims to be
- Consider **multiple contexts** (IP, location, login events, browser, behavior, ...)
- Calculate the **overall risk score** and assign it to **risk level**

Risk-based authentication

- **Evaluate risk** (probability) **the user is imposter** - not who claims to be
- Consider **multiple contexts** (IP, location, login events, browser, behavior, ...)
- Calculate the **overall risk score** and assign it to **risk level**
- **Risk level** (category) represents the magnitude of the risk



Risk-based authentication

- **Evaluate risk** (probability) **the user is imposter** - not who claims to be
- Consider **multiple contexts** (IP, location, login events, browser, behavior, ...)
- Calculate the **overall risk score** and assign it to **risk level**
- **Risk level** (category) represents the magnitude of the risk

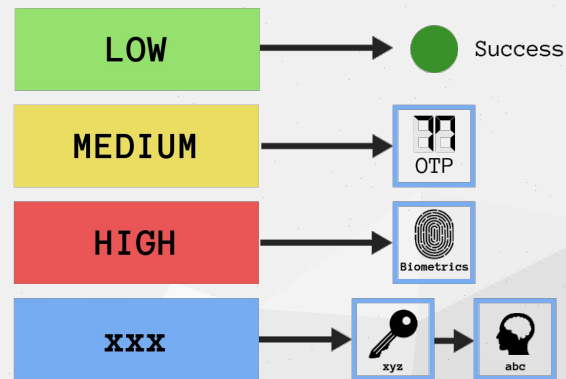
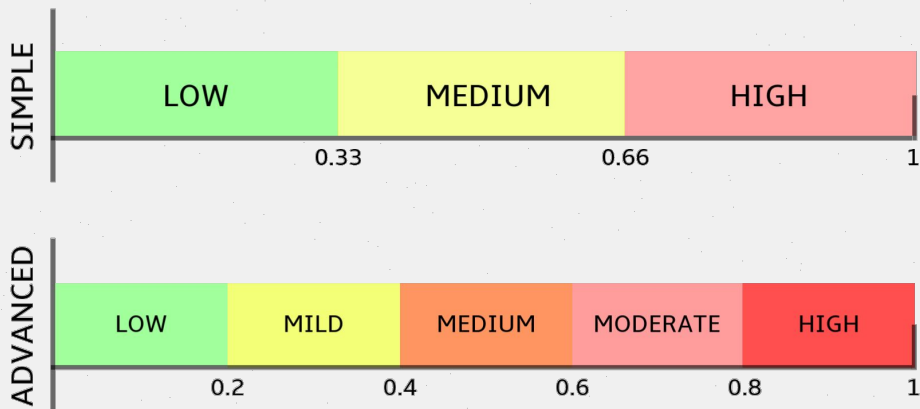
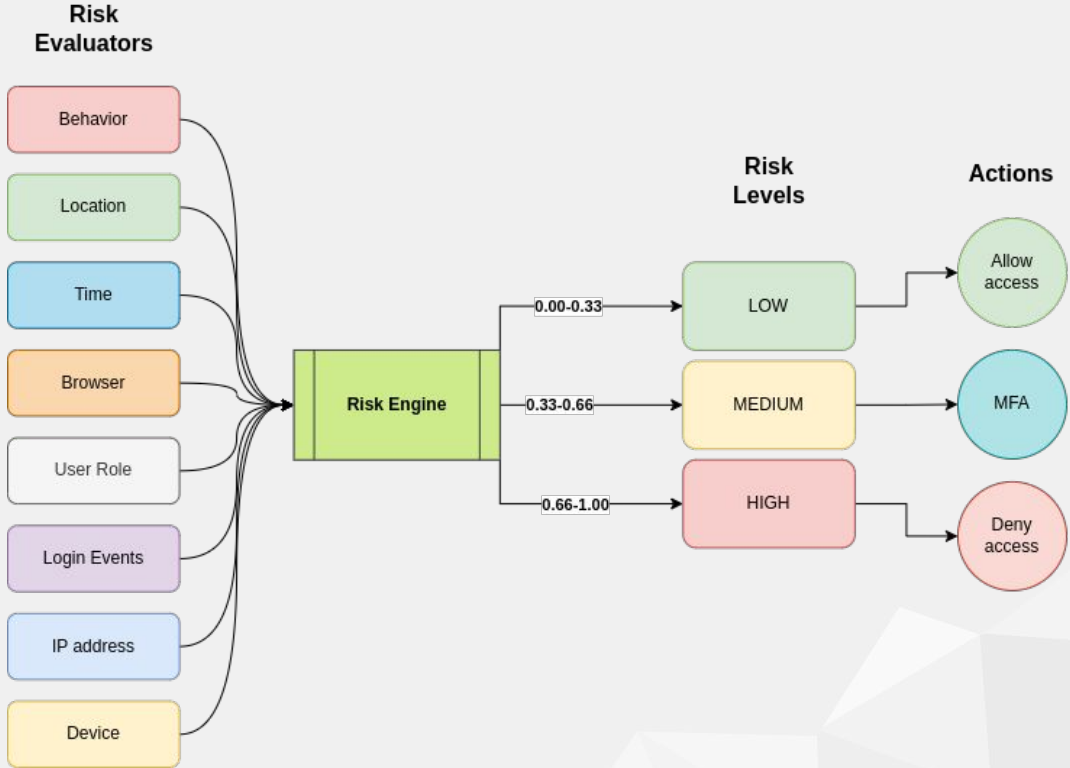


Figure 2. Risk levels

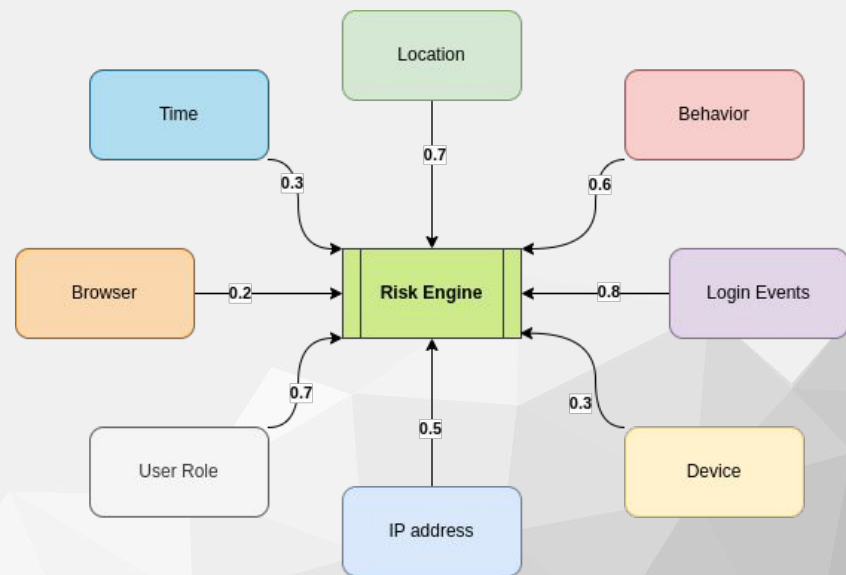
Risk score evaluation flow



Risk score **calculation**

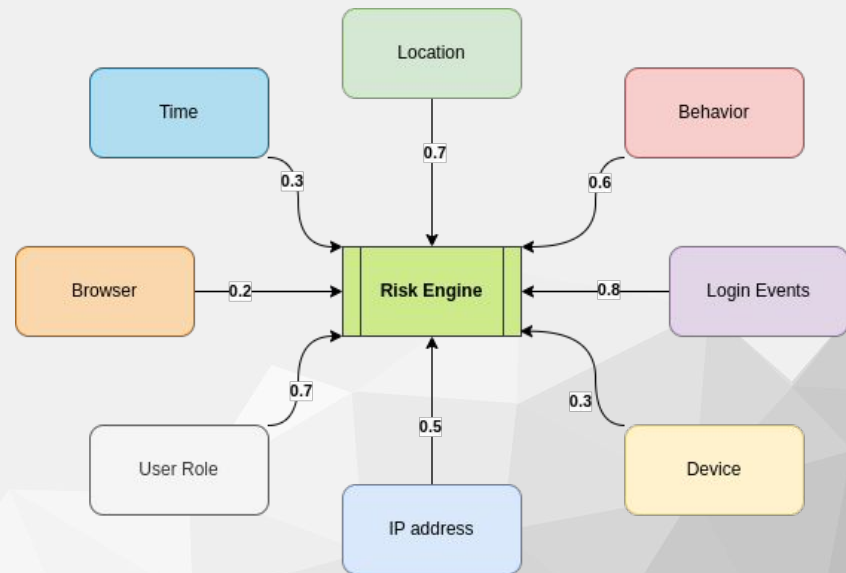
Risk score calculation

- Multiple **risk evaluators** for multiple contexts



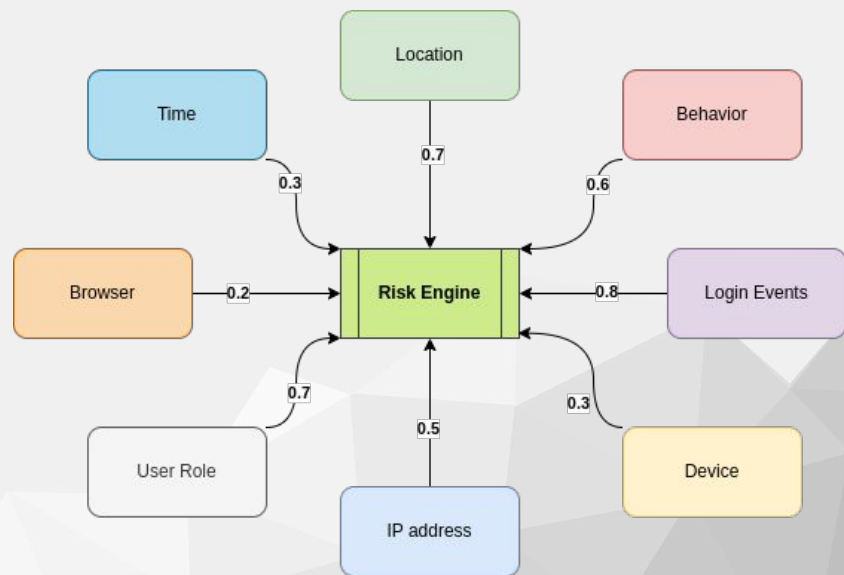
Risk score calculation

- Multiple **risk evaluators** for multiple contexts
- Risk evaluator evaluates risk for **specific context**



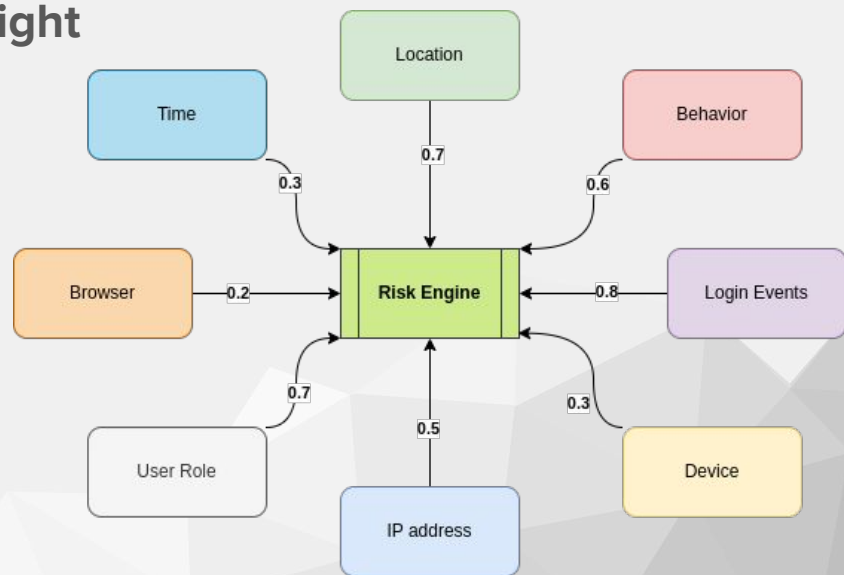
Risk score calculation

- Multiple **risk evaluators** for multiple contexts
- Risk evaluator evaluates risk for **specific context**
- Risk evaluator **requires user or not**



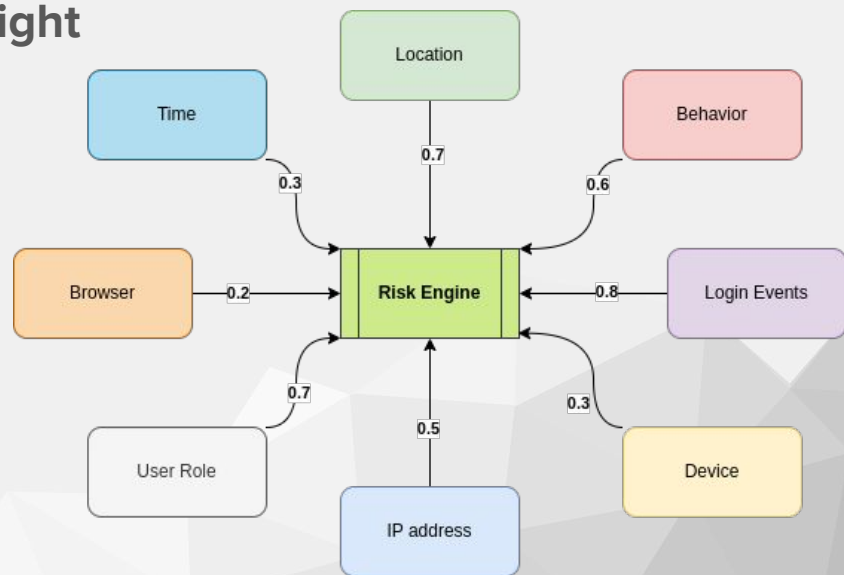
Risk score calculation

- Multiple **risk evaluators** for multiple contexts
- Risk evaluator evaluates risk for **specific context**
- Risk evaluator **requires user or not**
- Risk evaluator defines **risk score** and **weight**



Risk score calculation

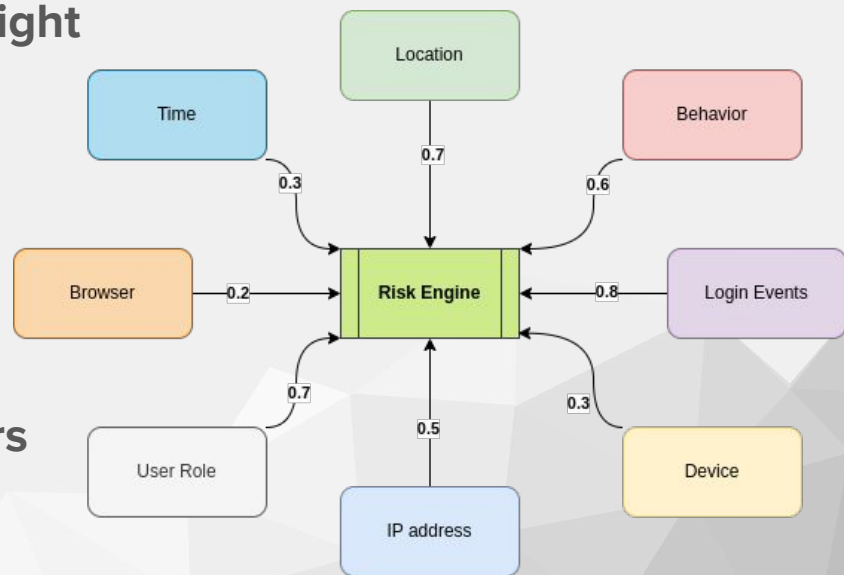
- Multiple **risk evaluators** for multiple contexts
- Risk evaluator evaluates risk for **specific context**
- Risk evaluator **requires user or not**
- Risk evaluator defines **risk score** and **weight**
- Weight represents how much the risk score should **influence** the **overall risk score**



Risk score calculation

- Multiple **risk evaluators** for multiple contexts
- Risk evaluator evaluates risk for **specific context**
- Risk evaluator **requires user or not**
- Risk evaluator defines **risk score** and **weight**
- Weight represents how much the risk score should **influence** the **overall risk score**

Overall risk = Weighted avg of risk evaluators



AI/ML Approach

AI/ML

- Artificial Intelligence for **more complex risk evaluations**

AI/ML

- Artificial Intelligence for **more complex risk evaluations**
- Leveraging **Natural Language Processing (NLP)** engines

AI/ML

- Artificial Intelligence for **more complex risk evaluations**
- Leveraging **Natural Language Processing (NLP)** engines
- Ability to **dynamically** evaluate risk score based on **multiple contexts**

AI/ML

- Artificial Intelligence for **more complex risk evaluations**
- Leveraging **Natural Language Processing (NLP)** engines
- Ability to **dynamically** evaluate risk score based on **multiple contexts**
- Returns the **risk score** and **calculation explanation**

AI/ML

- Artificial Intelligence for **more complex risk evaluations**
- Leveraging **Natural Language Processing (NLP)** engines
- Ability to **dynamically** evaluate risk score based on **multiple contexts**
- Returns the **risk score** and **calculation explanation**

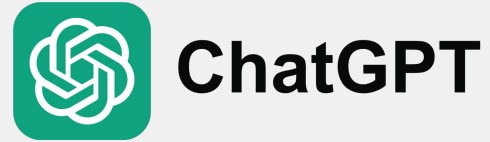
Use cases

- Processing logging events/logs
- Determine behavior change
- Geolocation analysis, impossible travel, ...

Current Approach

Current Approach

- Leveraging **OpenAI ChatGPT**



Current Approach

- Leveraging **OpenAI ChatGPT**
- Possibility to integrate **with any** AI model (NLP Engine)



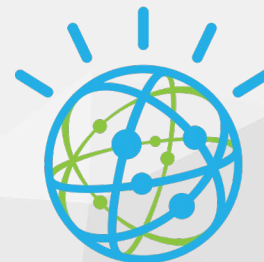
ChatGPT



Red Hat
OpenShift AI



Hugging Face



IBM Watson

Current Approach

- Leveraging **OpenAI ChatGPT**
- Possibility to integrate **with any** AI model (NLP Engine)
- **No custom model** for risk assessment **yet**



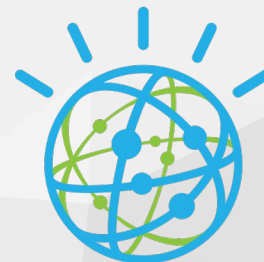
ChatGPT



Red Hat
OpenShift AI



Hugging Face



IBM Watson

Current Approach

- Leveraging **OpenAI ChatGPT**
- Possibility to integrate **with any** AI model (NLP Engine)
- **No custom model** for risk assessment **yet**
- **No wider context** about the authentication



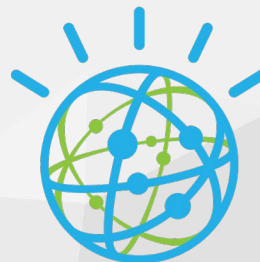
ChatGPT



Red Hat
OpenShift AI



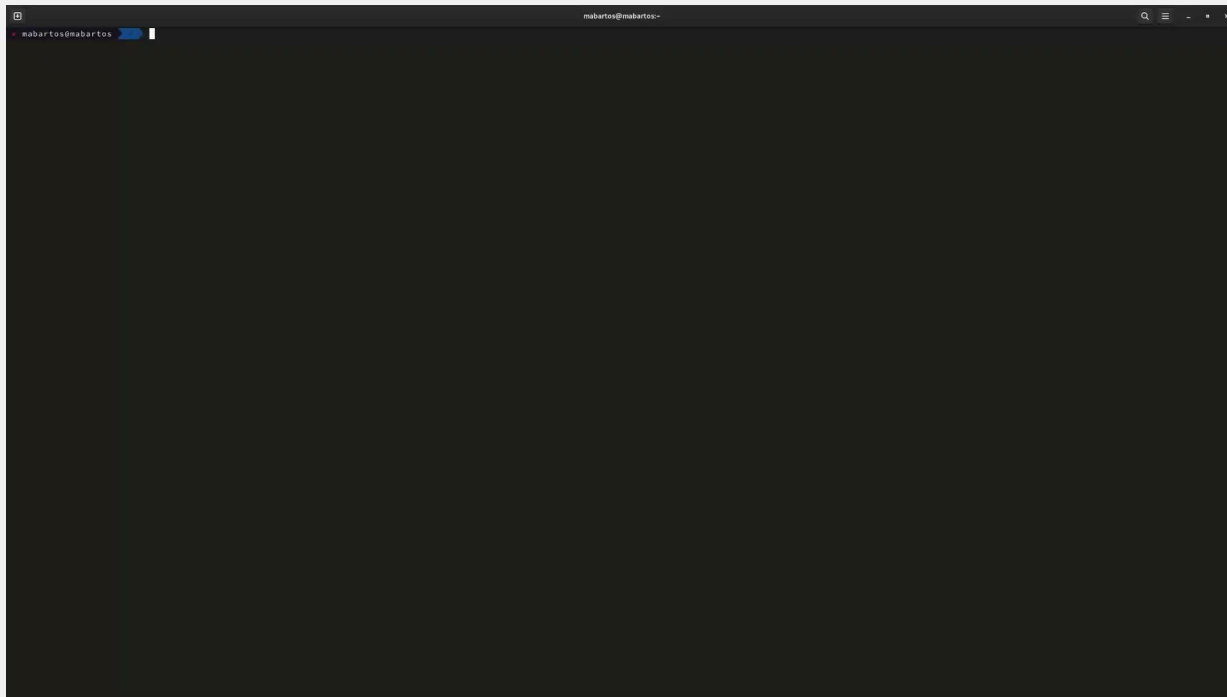
Hugging Face



IBM Watson

Demo

Demo



[Other link](#)

What next?

What next?

- Custom **AI models** - more efficient, more accurate, contextual
- **Continuous** risk evaluation
- More context information
- Keycloak focus group (?)
- Polishing, validations, ...

Stay in touch

Martin Bartoš

mabartos@redhat.com



Become a contributor:



[Keycloak Adaptive Authentication Extension](#)



@mabartos



@mabartos98

Credits

- *Figure 1. MFA vs Adaptive authentication. Source: <https://rublon.com/adaptive-authentication/>*
- *Figure 2. Risk levels. Inspired in <https://rublon.com/adaptive-authentication/>*
- *Icons: <https://www.flaticon.com/>*