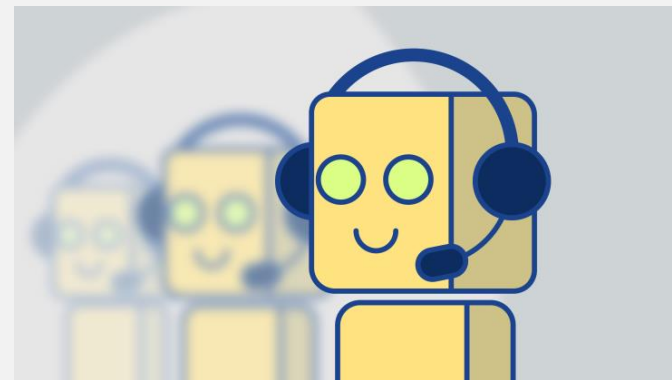


TECHNOLOGIE AGENTOWE: BOTY

Patryk Fulara, Michał Habigier, Andrzej Horowski

BOT

- Boty to programy służące do wykonywania określonych czynności przez maszynę na polecenie człowieka. Czasem ich funkcją jest udawanie ludzkiego zachowania. Nazwa **bot** pochodzi od słowa robot.
- Mogą mieć postać np. aplikacji, która po uprzedni ustawieniu będzie np. informować na bieżąco o zmianach pogody czy utrudnieniach w komunikacji miejskiej. Przykładami botów mogą być Siri (Apple), Cortana (Microsoft) czy Google Now czyli inteligentny osobisty asystent, który potrafi odpowiadać na pytania, wykonywać polecenia w systemie oraz wskazywać informacje, które uzna za przydatne użytkownikowi. Ta ostatnia funkcja dostępna jest poprzez zbieranie informacji o użytkowniku (lokalizacji GPS, wyszukiwane hasła).
- Mianem bota określa się także program (zwłaszcza w grach typu FPP), który wyręcza gracza w celowaniu i strzelaniu (tzw. aimbot). Boty można również spotkać w grach MMORPG, gdzie są używane do automatyzowania czynności wykonywanych przez gracza (np. ciągłe zabijanie potworów).
- Przykładem komercyjnego wykorzystania botów są automatyczni asystenci obsługujący klientów on-line (Chatboty). Są oni głównie wykorzystywani przez organizacje do komunikacji z konsumentami i użytkownikami usług.

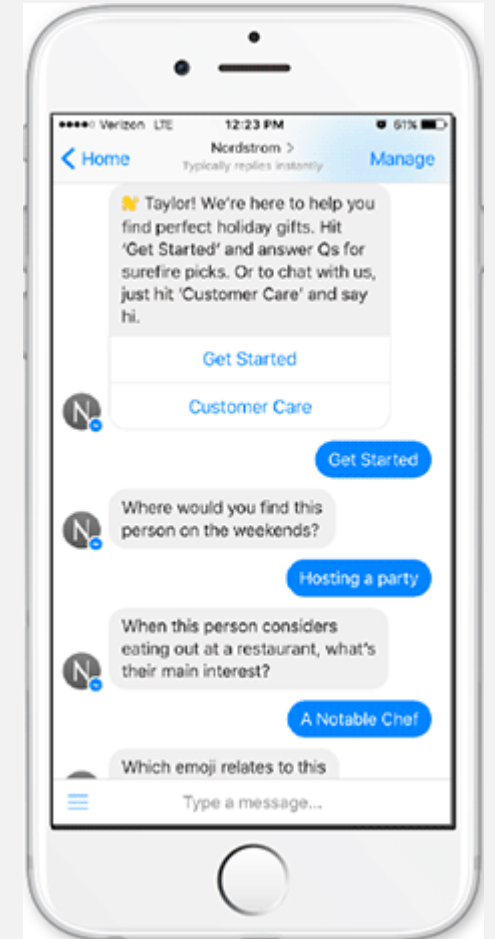


PODZIAŁ BOTÓW

- Infoboty - gromadzące i później udostępniające rozmaite informacje (dane statystyczne kanału, boty tworzące bazy danych użytkowników).
- Boty usługowo-specjalistyczne - są rodzajem łącznika między rozbudowanym programem a określonym kanałem IRC, np. chatbot.
- Boty “rozrywkowe” - boty do przeprowadzania quizów, gier, boty z bibliotekami żartów.
- Boty “serwery plików” - spełniają rolę serwerów FTP - udostępniają zasoby plików multimedialnych.
- Boty “nadzorcy” - najczęściej spotykane - służą do ochrony i pilnowania porządku w kanałach.

CHATBOT

- **Chatbot (chatterbot)** – program komputerowy, którego zadaniem jest prowadzenie konwersacji przy użyciu języka naturalnego bądź interfejsu tekstowego i sprawianie wrażenia inteligentnego. Zabieg ten ma na celu oszukanie rozmówcy, tak aby myślał, iż rozmawia on z żywym człowiekiem. Najpopularniejszym klasycznym chatbotem jest ELIZA zaprojektowana w 1966 roku jako program symulujący psychoanalityka, który parodiował terapeutę.
- Najprostsze chatboty posługują się stałą bazą wiedzy złożoną ze słów kluczowych i przypisanych im komunikatów, które wysyłają w odpowiedzi użytkownikowi, gdy w jego tekście znajdą dane słowo. Przykładowy prosty czatbot dostając pytanie "Jaka jest u ciebie pogoda?" mógłby odpowiadać komunikatem "Jest bardzo słonecznie" przypisanym do słowa "pogoda".
- Inną metodą używaną przez bota **ELIZA** jest nieznaczną zamianę wiadomości otrzymanej i odesłanie jej z powrotem. Przykładowo, jeśli rozmówca wysła "Nie jest dobrze", program może łatwo zamienić to na pytanie "Dlaczego nie jest dobrze?" i odesłać. Bardziej zaawansowane chatboty poszerzają swoją bazę wiedzy w trakcie kolejnych rozmów.



AIML

Język znaczników oparty na języku XML, służący do tworzenia baz wiedzy chatterbotów.

Język ten zawiera kilka różnych elementów.

- Kategorie `<category>` są najważniejszymi znacznikami AIML. Kategorie składają się z przynajmniej dwóch elementów: znacznika `<pattern>` oraz znacznika `<template>`
- Wzorzec `<pattern>` jest ciągiem znaków dopasowanych do jednego lub więcej zapytań użytkownika.

JAK MASZ NA IMIĘ

*JAK MASZ **

- Szablony `<template>` określają reakcje na wzorzec. Szablony mogą być całą odpowiedzią.

```
<aiml version="1.0.1">
  <category>
    <pattern>HELLO</pattern>
    <template>Witam.</template>
  </category>
</aiml>
```

```
<category>
  <pattern>JAK MASZ NA IMIĘ</pattern>
  <template>MAM NA IMIĘ <bot name="name"/>.</template>
</category>
<category>
  <pattern>JAK SIĘ NAZYWASZ</pattern>
  <template>
    <srai>JAK MASZ NA IMIĘ</srai>
  </template>
</category>
```

ZASTOSOWANIE CHATBOTÓW

- **Boty dla biznesu**

Ze względu na rosnący problem niedoboru pracowników to będzie najszybciej rozwijający się kierunek wykorzystania sztucznej inteligencji AI. Przy pomocy chatbotów możemy zamówić swoje ulubione danie, kupić buty, wybrać książkę czy film na wieczór. To właśnie działy obsługi klienta i telemarketingu mogą bardzo szeroko wykorzystywać boty w procesie komunikacji od momentu przedstawienia oferty produktów, poprzez rekomendacje na informacjach o dostawie kończąc. Innym sposobem wykorzystania botów są procesy związane z księgowością. Boty do wystawiania faktur mogą poprawić efektywność oraz zminimalizować liczbę pomyłek.

- **Boty dla służby zdrowia**

Wykorzystanie tej technologii pozwoli bardzo łatwo wybrać odpowiedniego lekarza i zebrać opinię na jego temat, umówić wizytę czy sprawdzić jaki zakres działania ma konkretna placówka oraz wskazać w jaki sposób powinno się stosować leki.

Wirtualny asystent medyczny - aplikacje z botami w przyszłości pomogą również odnaleźć najbliższą otwartą aptekę czy gabinet dentystyczny.

- **Boty dla turystyki**

Wirtualny przewodnik - może towarzyszyć nam w zwiedzaniu nowych miejsc, opowiedzieć ich historię wskazać ciekawostki i anegdoty z nimi związane. Będzie do naszej dyspozycji 24/7 właśnie wtedy kiedy będziemy chcieli skorzystać z jego pomocy. AI może być wykorzystywana do wsparcia biur informacji turystycznej, jako pomoc w wyszukiwaniu i rezerwacji pokoi hotelowych oraz innych miejsc potrzebnych w podróży jak restauracje czy stacje paliw itd. Chatboty mogą pomagać również w wyszukiwaniu połączeń lotniczych i bookowaniu biletów.

BOTY W GRACH

W grach wideo bot jest rodzajem oprogramowania systemu AI, który gra w grę wideo zamiast człowieka. Boty są wykorzystywane w różnych gatunkach gier wideo do różnych zadań: bot napisany do strzelanki FPS działa inaczej niż ten napisany dla gry MMORPG. Te pierwsze mogą obejmować analizę mapy, a nawet podstawową strategię; ten ostatni może być wykorzystywany do automatyzacji powtarzalnych i żmudnych zadań.

Boty napisane dla strzelanek pierwszoosobowych zazwyczaj starają się naśladować sposób, w jaki człowiek zagrałby w grę. Boty sterowane komputerowo mogą grać w pojedynkę z innymi botami i / lub graczami. Funkcje i inteligencja botów mogą się znacznie różnić. Zaawansowane boty posiadają uczenie maszynowe do dynamicznego uczenia się wzorców przeciwnika, a także dynamicznego uczenia się wcześniej nieznanych map - podczas gdy bardziej trywialne boty mogą całkowicie polegać na listach punktów tworzonych dla każdej mapy przez programistę, ograniczając bota do odtwarzania tylko map z wspomnianymi punktami trasy.

Boty statyczne są zaprojektowane tak, aby śledzić gotowe punkty na każdym poziomie lub mapie. Te boty muszą mieć unikalny plik punktów drogi dla każdej mapy, jeśli mają funkcjonować.

Dynamiczne boty, uczą się poziomów i map podczas ich gry.





Mianem bota określa się także program, który automatycznie ustawia celownik broni na przeciwników znacząco ułatwiając grę osobie korzystającej z tego programu – musi ona tylko nacisnąć przycisk. (aimbot)

BOTY – ROSNĄCE ZAGROŻENIE

- Boty są obecnie jednym z najbardziej złożonych i popularnych rodzajów przestępczości internetowej. Pozwalają hakerom na przejęcie kontroli nad wieloma komputerami jednocześnie i przekształcenie ich w komputery „zombi”, które działają jako część potężnej sieci typu „bot” służącej do rozsyłania wirusów, generowania spamu oraz dokonywania innych przestępstw i oszustw internetowych.
- Zanim komputer zainfekowany botem wykona polecenie od głównego bota, wiele osób określa taki komputer mianem „zombi”. Przestępców internetowych, którzy kontrolują te boty, nazywa się botmasterami (używane jest także określenie botherder).
- Niektóre sieci typu „bot” mogą obejmować kilkaset lub kilka tysięcy komputerów, podczas gdy inne dysponują dziesiątkami lub nawet setkami tysięcy komputerów „zombi”. Wiele z tych komputerów jest zainfekowanych bez wiedzy ich właścicieli. Jakie są możliwe sygnały ostrzegawcze? Bot może spowalniać pracę komputera lub prędkości łącza, powodować wyświetlanie tajemniczych komunikatów lub nawet prowadzić do awarii komputera.
- Boty przenikają do komputerów na wiele sposobów. Często rozprzestrzeniają się w Internecie, wyszukując niechronione komputery, które można zainfekować przez wykorzystanie luk w zabezpieczeniach. Po znalezieniu celu ataku boty szybko infekują komputer, a następnie wysyłają raport do głównego bota. Później pozostają w ukryciu do momentu otrzymania polecenia wykonania jakiegoś zadania.

BOTY – DZIAŁANIA NIEPOŻĄDANE

Komputer przejęty przez bota może zostać użyty do przeprowadzenia różnorodnych zautomatyzowanych zadań takich jak:

Rozsyłanie	Kradzieże	Ataki typu DdoS	Fałszywe kliknięcia
			
Boty mogą rozsyłać: <ul style="list-style-type: none">— spam— wirusy— programy typu „spyware”	Umożliwiają wykradanie informacji osobistych w celach przekazania ich osobom nieupoważnionym o wrogich zamiarach: <ul style="list-style-type: none">— numery kart kredytowych— informacje dające dostęp do kont bankowych— inne poufne dane osobiste	Służą do przeprowadzania ataków typu „odmowa usługi” (DdoS, Distributed denial of Service) na określony cel. Przestępcy internetowi wyłudniają pieniądze od właścicieli witryn internetowych w zamian za odzyskanie kontroli nad zaatakowanymi witrynami.	Oszuści używają botów w celu zwiększenia przychodów z reklam internetowych przez automatyczne klikanie reklam.

OCHRONA PRZED BOTAMI

Aby ochronić się przed niepożądanymi działaniami botów należy przede wszystkim:

- Korzystając z internetu kierować się zdrowym rozsądkiem za czym idzie nieodwiedzanie nieznanym lub podejrzanych stron czy też tych niezabezpieczonych odpowiednim protokołem
- Nie otwierać załączników od nieznanych nadawców oraz załączników o podejrzanej treści
- Dbać o aktualizację oprogramowania antywirusowego oraz oprogramowań, które mogą posiadać luki bezpieczeństwa



Programiści powinni z kolei stosować automatyczne metody takie jak np.:

- captcha
- pytania logiczne/matematyczne
- weryfikacja adresu e-mail
- wszystkie powyższe razem
- zezwolenie na korzystanie z pełnej funkcjonalności serwisu po pewnym czasie od rejestracji