



Mariusz Dziechciaronek, Piotr Jordanowski, Natalia Bednarz

**Czy aby na pewno jest Pan człowiekiem?
Użyteczność kodów CAPTCHA.**

Dane adresowe

Symetria
Agencja e-biznes i dom mediowy
ul. Wyspiańskiego 10/4
60-749 Poznań

Kontakt

tel.: 061 864 36 55
faks: 061 864 36 55
e-mail: symetria@symetria.pl
www.symetria.pl

SPIS TREŚCI:

1.	Wprowadzenie	3
2.	Maszyna udająca człowieka	4
3.	Halo? Czy na pokładzie jest człowiek?	5
4.	?[!:>@_{};.....CAPTCHA!	6
5.	A czy Ty też jesteś content?	9
6.	Zabezpiecz się!	11
7.	Test z człowieczeństwa	14
8.	Podsumowanie.....	21
9.	Kilka słów o Symetrii	23

1. Wprowadzenie

Ile razy każdy z nas wpisywał po raz kolejny i kolejny kod z obrazka, próbując założyć nowe konto pocztowe, albo dokończyć proces rejestracji. Najbardziej zniechęceni przez użytkowników i często obrzucani najgorszymi epitetami kody CAPTCHA strzegą bezpieczeństwa serwisów, a raczej strzegły ich bezpieczeństwa. Po złamaniu kodów CAPTCHA Google na początku zeszłego roku, żaden kod weryfikacyjny nie jest już bezpieczny. Coraz bardziej zaawansowane oprogramowanie OCR, stanowi narzędzie do zarabiania grubych milionów przez „biznesmanów” zainteresowanych rozsyłaniem na cały świat spamu.

Agencja e-biznes Symetria przeprowadziła prekursoryczne na polskim rynku badania użyteczności kodów weryfikacyjnych typu CAPTCHA. W badaniu zostały przeanalizowane kody zabezpieczające trzech czołowych serwisów internetowych:

- **Gazeta.pl,**
- **o2.pl,**
- **Youtube.**

Kody tego typu występują w formularzach rejestracyjnych, przy zakładaniu kont pocztowych, czy dodawaniu komentarzy do artykułu lub postów do bloga. Kod ma zwykle postać liter lub cyfr, które należy przepisać z obrazka.

Symetria przeprowadziła badania eye trackingowe (śledzenie ruchu gałek użytkownika) długości czasu i ilości spojrzeń niezbędnych do prawidłowego wpisania kodu CAPTCHA.

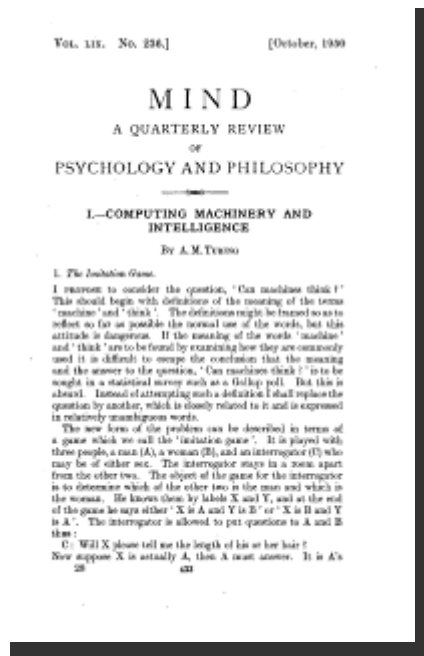
Wnioski z badania stanowią zbiór konkretnych rekomendacji w zakresie budowy użytecznych, przyjaznych dla użytkownika kodów CAPTCHA.

W poniższym artykule zawarte zostały informacje wprowadzające na temat kodów CAPTCHA, ich znaczenia, zastosowania i niebezpieczeństw związanych z ich implementacją. W drugiej części artykułu omówione zostały przeprowadzone przez Symetrię badania eye trackingowe kodów weryfikacyjnych.

2. Maszyna udająca człowieka

W 1950 roku angielski matematyk **Alan Turing** zaproponował rodzaj gry logicznej, której celem była próba odpowiedzi na pytanie, do jakiego momentu możemy twierdzić, że dany układ logiczny jest inteligentny.

W swej podstawowej wersji **Test Turinga** polega na symulowaniu rozmowy między trzema podmiotami, z których jeden jest komputerem. Jeśli po upływie określonego czasu ludzcy rozmówcy nie będą w stanie określić, czy prowadzili rozmowę z człowiekiem czy z maszyną, wówczas stanowić to będzie dowód na to, że komputer jest inteligentny.



Rysunek 1 Pierwsza strona publikacji Computing Machinery and Intelligence A.Turinga; <http://www.jstor.org/pss/2251299>.

3. Halo? Czy na pokładzie jest człowiek?

CAPTCHA to nic innego jak kod weryfikacji człowieczeństwa. Z założenia stanowić ma barierę dla botów i oprogramowania czytającego i łamiącego kody - **OCR (ang. Optical Character Recognition)**.

Jednym słowem jeśli jesteś botem, powinieneś przynajmniej w teorii mieć problem z założeniem konta w popularnym serwisie, czy ściągnięcia najnowszych poprawek do Linuksa na swój dysk. Rzeczywistość wygląda jednak inaczej. Z jednej strony serwisy walczą o utrzymanie minimalnych standardów bezpieczeństwa, z drugiej zaś próbują nie narazić się zbyt wielu użytkownikom.

Nazwę **CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart)** zaproponowali po raz pierwszy Luis von Ahn, Manuel Blum, Nicholas J. Hopper z Carnegie Mellon University.



Rysunek 2 Luis von Ahn; http://en.wikipedia.org/wiki/File:Wikipedia_luis.jpg

Proste kody CAPTCHA są bardzo łatwe do hackowania, rzecz jasna łamanie kodów musi być opłacalne, tj. czas złamania jednego kodu powinien być na tyle niski, aby móc hackować kody masowo. W przeciwnym wypadku łamanie kodu będzie tylko sztuką dla sztuki, a nie przykładem ciekawego sposobu na nielegalny zysk.

4. ?[!:>@_{};.....CAPTCHA!

Z CAPTCHA od samego początku jego istnienia był problem. Problem ten narastał latami, budując coraz to nowe bariery dla użytkownika.

Główne problemy użyteczności CAPTCHA:

- niska rozpoznawalność przez użytkownika,
- skomplikowanie samego kodu – zadania matematyczne, itp.,
- problemy z odczytaniem kodu CAPTCHA przez osoby niepełnosprawne: niewidzące, niedowidzące, niesłyszące, cierpiące na inne problemy,
- brak przycisku odśwież kod – automatyczne przeładowanie strony i utrata danych z formularza,
- brak informacji dlaczego należy wpisać CAPTCHA,
- brak przycisku Audio,
- brak alternatywnej poza sieciowej identyfikacji użytkownika przez serwis – takie usługi zapewnia Yahoo.

Użyteczność CAPTCHA może być rozpatrywana w wielu aspektach. Najważniejsze z nich zostały posegregowane przez naukowców, którzy zawodowo zajmują się hackowaniem kodów – Jiefa Yan, Ahmada Ahmad, w pracy [Usability of CAPTCHAs or Usability Issues in CAPTCHA Design](#)

Table 1. Usability issues with text-based CAPTCHAs

Category	Usability issue	
Distortion	Distortion method and level	
	Confusing characters	
	Friendly to foreigners?	
Content	Character set	
	String length	How long?
		Predictable or not?
	Random string or dictionary word?	
	Offensive word	
Presentation	Font type and size	
	Image size	
	Use of colour	
	Integration with web pages	

Rysunek 3 J. Yan, A. Ahmad, Usability of CAPTCHAs or Usability Issues in CAPTCHA Design;
<http://cups.cs.cmu.edu/soups/2008/proceedings/p44Yan.pdf>.

Distortion – czyli celowe zaburzanie elementów kodu, tak aby oprogramowanie OCR miało problem z jego czytaniem, stanowi podstawowy i najważniejszy aspekt bezpieczeństwa CAPTCHA. Do niedawna kody Google, dzięki zastosowaniu techniki **stłaczania liter (crowded)** stanowiły nie lada problem dla botów. W celu zarabiania na ich łamaniu, wspomniani wcześniej „biznesmani” zmuszeni byli do wynajmowania Hindusów czy Chińczyków, którzy rozpoznawali i wpisywali miliony kodów każdego dnia.

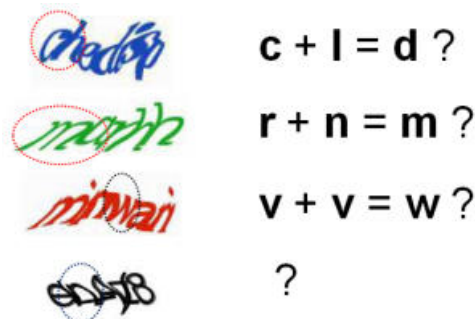
Mimo, że nie ma obecnie w pełni zabezpieczonych przed atakiem kodów tekstowych CAPTCHA, to wciąż jeszcze ten sposób weryfikacji użytkownika jest bardzo popularny. W tym miejscu należy również nadmienić, że nie każde oprogramowanie OCR jest od razu zdolne do czytania i łamania skomplikowanych kodów.

Do najważniejszych zaburzeń zaliczamy:

- przemieszczanie elementów w górę i w dół,
- obroty elementów,
- skalowanie elementów,
- gięcie elementów.



Rysunek 4 Budowa CAPTCHA



Rysunek 5 Problemy z odczytaniem zaburzonego kodu

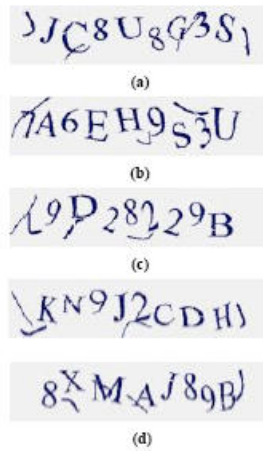


Figure 1. Microsoft CAPTCHA: the 1st object in (a), (b) and (c) looks like 'J', '7' and 'L' respectively. The last object in each image in (d) looks like 'J'.

Rysunek 6 Kody CAPTCHA Microsoftu, J. Yan, a. Ahmad, Usability of CAPTCHAs or Usability Issues in CAPTCHA Design; <http://cups.cs.cmu.edu/soups/2008/proceedings/p44Yan.pdf>

Microsoft w swoich wcześniejszych wersjach kodów CAPTCHA stosował trudne do rozpoznawania łuki, które miały wprowadzać w błąd oprogramowanie OCR, traktujące zaburzające elementy (distortion clutter) jako elementy rzeczywistego kodu.

5. A czy Ty też jesteś content?

Kolejnym elementem, który ma przysporzyć udręki użytkownikowi jest **content kodu**. Tutaj istotną rolę odgrywa wielkość elementów i ich ilość czyli **string**. Badania pokazują, że im większy element, tym wyższe bezpieczeństwo, ale i większe prawdopodobieństwo ponadnormatywnego zaburzenia elementów kodu, który może się stać nieczytelny dla użytkownika.

Dobrą praktyką ułatwiającą życie użytkownikom jest podanie liczby elementów, które należy wpisać w polu weryfikacji. Zwykle taka informacja nie wpływa negatywnie na poziom bezpieczeństwa kodu.

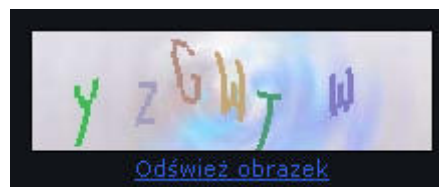


Rysunek 7 Sympatia.pl podaje ilość znaków do wpisania.

Sporną kwestią pozostaje to, czy CAPTCHA powinno generować istniejące słowa czy tylko zbiory przypadkowych znaków. Yan i Ahmad argumentują, że nie ma to znaczenia, jednocześnie zastrzegając, że używanie słów nieistniejących, lub odmiennych od danego obszaru kulturowego implikuje problemy użyteczności.

Prezentacja kodu jest równie ważna z perspektywy użyteczności jak poziom zaburzeń elementów. Nieprofesjonalne używanie koloru, tworzenie mozaik kolorów tła, wprowadzania wielu odcieni, jest często barierą nie do przejścia dla użytkownika. OCR radzi sobie z takimi przeszkodami bardzo dobrze.

Zatem jeśli nie jesteś ekspertem, używaj tylko dwóch kolorów, nie staraj się tworzyć obrazów Kandinskiego bo stracisz swoich użytkowników.



Rysunek 8 CAPTCHA w serwisie PEB

Dostępność CAPTCHA to kolejny problem. Do niedawna dostępne dla niewidzących użytkowników były tylko kody Google i reCAPTCHA. Dziś mamy więcej przyjaznych serwisów dla niepełnosprawnych. Aczkolwiek problem prawidłowego odsłuchania kodu, może czasem stanowić nie lada wyzwanie, szczególnie jeśli nie jest się rodowitym Teksasńczykiem czy mieszkańcem Dover.



Rysunek 9 reCAPTCHA

E-mail

Hasło:

Wpisz znaki widoczne na poniższym obrazku.



&

Wielkość liter nie jest brana pod uwagę

Rysunek 10 Google CAPTCHA z możliwością odsłuchania kodu

Dobre praktyki AUDIO CAPTCHA:

- możliwość odsłuchania CAPTCHA to warunek dostępności,
- zaburzenie tła dźwiękowego musi być ograniczone,
- obecność znaczka audio/niepełnosprawni,
- rozsądne stosowanie javascript i flash.

[Odsłuchaj audio Google CAPTCHA](#)

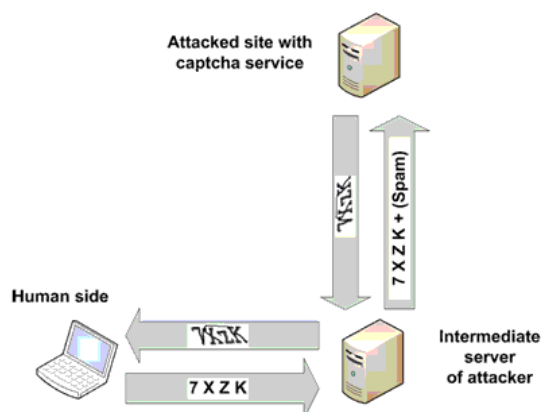
6. Zabezpiecz się!

CAPTCHA nie jest zbyt trudne do złamania w dzisiejszych czasach. Problem polega na opłacalności nielegalnej działalności. Jeśli tylko zaangażowanie się w działanie polegające na łamaniu kodu, ma ostatecznie doprowadzić do „zwrotu z inwestycji” to na pewno znajdą się ludzie, którzy wykorzystają słabości CAPTCHA.

Jak można łamać CAPTCHA:

- wykorzystanie oprogramowania OCR (Optical Character Recognition),
- analiza statystyczna – słów i obrazów z bazy danych CAPTCHA,
- sieci neuronowe, znacznie lepsze od klasycznych podejść algorytmicznych w rozpoznawaniu kształtów,
- farma Turinga, czyli zatrudnienie w jakimś kraju Trzeciego Świata setek ludzi, którzy będą rozwiązywali przedstawiane im CAPTCHA,
- farma porno Turinga – czyli spamer zakłada stronę „tylko dla dorosłych”, w której warunkiem obejrzenia pornograficznego obrazka jest zdekodowanie CAPTCHA pochodzącej z innej strony.

Poniżej zaprezentowano bardzo ciekawy pomysł na nielegalny biznes (farma porno Turinga) koncepcja bazuje na wykorzystaniu obrazków pornograficznych do łamania kodów weryfikacyjnych. Na komputerze użytkownika instaluje się trojan, który wyświetla okno z rozebraną Panią. Dalsze części jej garderoby mogą znaleźć się na podłodze, jeśli tylko użytkownik wpisze poprawny kod CAPTCHA. Kod jest ściągany ze strony np. Yahoo, po wpisaniu, przez użytkownika kodu, Pani z obrazka jest bardziej roznegliżowana, a cyberprzestępca zakłada kolejne konto w serwisie z którego pobrał kod.



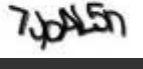
Rysunek 11 Działanie farmy porno Turinga; <http://pandalabs.pandasecurity.com/archive/A-new-way-of-social-engineering.aspx>:



Im więcej kodów CAPTCHA, tym mniej garderoby





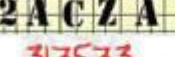

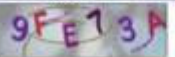

Rysunek 12 Przykład farmy porno Turinga; <http://www.heise-online.pl/security/Striptizowy-trojan--/news/item/1781>



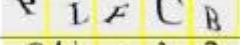





Genial	Yahoo!	Hotmail
		
		
		

Rysunek 13 Przykłady odpornych jeszcze do niedawna na ataki kodów CAPTCHA

Poniżej zaprezentowano, wskaźniki procentowe rozpoznawalności kodu przez OCR:

Editor	CAPTCHA	Success Percentage	Required Time
Google		20% 80%	6s 1min
Microsoft		15% 70%	6s 1min
Yahoo		30% 80%	6s 40s
Ebay		80%	4s
PayPal		100%	2s
Clubik		100%	1s
phoBB (forum)		97%	3s
IPB (forum)		97%	7s

Characters under typical distortions	Recognition rate
	~100%
	96-9%
	100%
	98%
	~100%
	95-9%

Rysunek 14 McAfee; http://vil.nai.com/images/FP_BLOG_081008_1.jpg

Rysunek 15 J. Yan, A. Ahmad, A low cost attack on a Microsoft CAPTCHA; http://homepages.cs.ncl.ac.uk/jeff.yan/msn_draft.pdf

7. Test z człowieczeństwa

Przeprowadziliśmy w Symetrii mały test użyteczności kodów weryfikacyjnych CAPTCHA za pomocą metody eye trackingowej. Do badania wybraliśmy trzy serwisy, których użyteczność kodów zabezpieczających chcieliśmy zweryfikować na podstawie danych otrzymanych w procesie rejestracyjnym.

1. Konto pocztowe Gazeta.pl.
2. Konto serwisu Youtube.pl.
3. Konto pocztowe O2.pl.

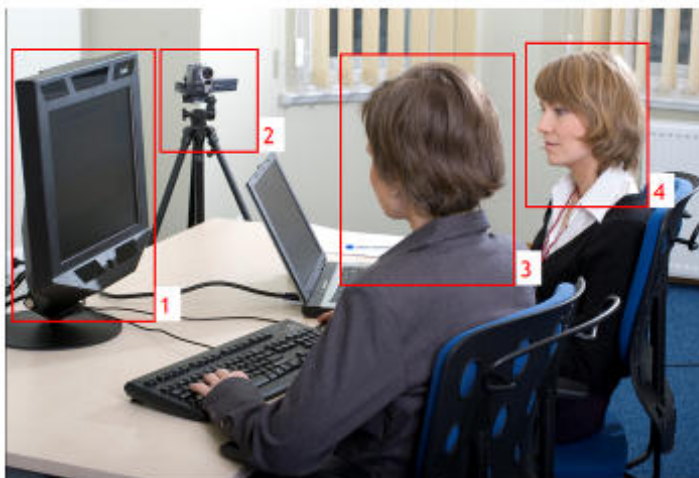
Zadania użytkownika polegały na:

1. Założeniu nowego konta pocztowego w serwisie Gazeta.pl.
2. Założeniu nowego konta w serwisie Youtube.pl.
3. Założeniu nowego konta pocztowego w serwisie O2.pl.

Czym jest eye tracking

Eye tracking to badanie ruchów gałek ocznych użytkownika w czasie trwania sesji badawczej. Badanie tego typu jest bezinwazyjne. Specjalne emitery podczerwieni śledzą ruch gałek ocznych użytkownika kiedy ten korzysta z serwisu.

Wzrok śledzony jest za pomocą urządzenia zwanego eye trackerem, które zastępuje w czasie badania monitor komputerowy i jest do niego łudząco podobne.



- 1 - eye tracker.
- 2 - kamera video rejestrująca reakcje badanego użytkownika.
- 3 - badany.
- 4 - specjalista ds. badania użyteczności/moderator.

Rysunek 16 Przykładowe badanie eye trackingowe wykonywane w agencji Symetria.

O badaniu

Z uwagi na dobro badania nie ujawnialiśmy jego prawdziwego celu, którym jest zbadanie rozpoznawalności i użyteczności kodów weryfikacyjnych CAPTCHA. Tak, aby badany użytkownik, nie skupiał całej swojej uwagi na prawidłowym odczytaniu kodu - a co za tym idzie aby nie wpływać na naturalne działania użytkownika.

W analizie danych dotyczących liczby spojrzeń w obszar CAPTCHA wzięto pod uwagę tylko i wyłącznie efektywne spojrzenia, a więc te, które prowadziły bezpośrednio do wpisania słowa z obrazka.

Poniżej zaprezentowano również wyniki analiz eye trackingowych w postaci tak zwanych gazeplotów, czyli ścieżek spojrzeń, obrazują one jak długo i w jakiej kolejności użytkownik patrzył na elementy strony.

Wiedza na ten temat daje nam możliwość przeprojektowania serwisu, eliminacji elementów nie spełniających swojej roli np. nie zwracających uwagi użytkownika. Z kolei fiksjacja jest to zatrzymanie się wzroku na jakimś elemencie strony, im większa średnica koła, tym dłuższy czas patrzenia użytkownika na dany element strony.

Uczestnicy badania

- kobiety i mężczyźni,
- wiek 20-30 lat,
- internauci,
- mieszkańcy miasta powyżej 500 tys. mieszkańców,
- zarówno osoby, które nie korzystały z tego typu serwisów, jak i takie, które miały z nimi kontakt.

Zastrzeżenie

Należy również nadmienić, że celem testu było zebranie inspiracji i przykładowych wniosków, nie było nim zaś jakiegokolwiek porównanie wybranych serwisów, ich test eye trackingowy ani szczegółowa analiza użyteczności i funkcjonalności.

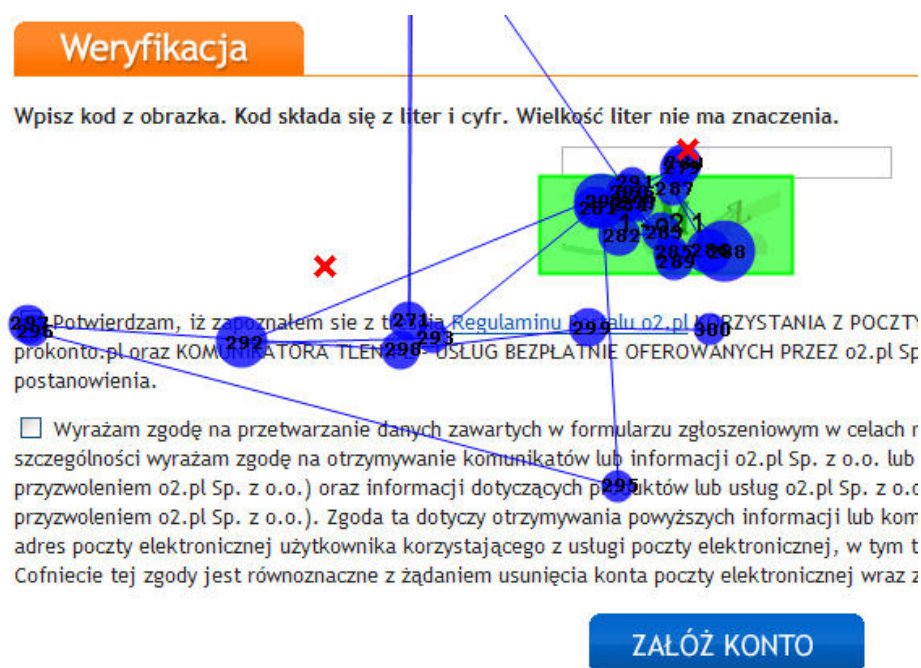
Omówione poniżej wyniki badania mają charakter eksperymentalny. Wyniki należy traktować jako inspirujące wskazówki do dalszych poszukiwań i weryfikacji w trakcie kolejnych badań.

Konto pocztowe O2.pl

Wpisz kod z obrazka. Kod składa się z liter i cyfr. Wielkość liter nie ma znaczenia.



Rysunek 17 CAPTCHA w serwisie O2.pl



Rysunek 18 Przykładowy gazeplot (ścieżki i czas spojrzeń) na kod CAPTCHA w serwisie o2.pl

Statystyka opisowa dla liczby fiksacji i łącznego czasu trwania fiksacji CAPTCHA zamieszczonego w serwisie o2.pl wskazuje na bardzo małą liczbę spojrzeń potrzebnych do wpisania słowa z obrazka.

Średnio użytkownicy potrzebowali 5 spojrzeń na przeczytanie obrazka, a aż 50% badanych potrzebowało mniej niż 3 spojrzeń. Z prawdopodobieństwem 95% można stwierdzić, że liczba spojrzeń potrzebnych na przeczytanie obrazka w populacji zmieści się pomiędzy 2 a 8.

Średni łączny czas trwania spojrzeń wyniósł niewiele ponad 1 sekundę, a połowa badanych potrzebowała mniej niż 0,6 sekundy na wpisanie kodu. Z prawdopodobieństwem 95% można stwierdzić, że w populacji łączny czas potrzebny na przeczytanie obrazka nie przekroczy 2,1 sekundy. Należy zwrócić uwagę, że w jednym przypadku osoba potrzebowała aż 14 spojrzeń, co znacznie zawiżyło średnią i zniekształciło miary skośności.

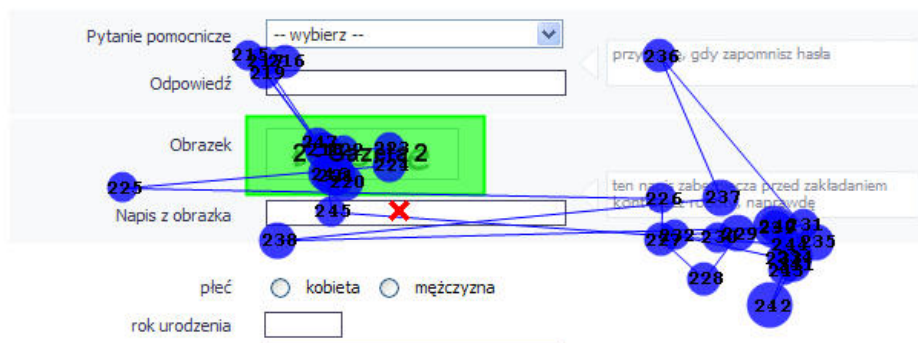
	<i>Liczba fiksacji</i>	<i>Łączny czas trwania fiksacji w ms</i>
Średnia	5	1173
Mediana	3	638
Odchylenie standardowe	4,07	1144,87
Wariancja próbki	16,57	1310725,71
Kurtoza	5,43	-0,12
Skośność	2,28	1,32
Minimum	2	279
Maksimum	14	3093
Poziom ufności(95,0%)	3	957

Rysunek 19 Dane statystyczne dla liczby spojrzeń i łącznego czasu spojrzeń na kod CAPTCHA w serwisie o2.pl

Konto pocztowe Gazeta.pl



Rysunek 20 CAPTCHA w serwisie Gazeta.pl



Rysunek 21 Przykładowy gazeplot (ścieżki i czas spojrzeń) na kod CAPTCHA w serwisie Gazeta.pl

Statystyka opisowa dla liczby fiksacji i łącznego czasu trwania fiksacji CAPTCHA zamieszczonego w serwisie Gazeta.pl wskazuje na umiarkowaną liczbę spojrzeń potrzebnych do wpisania słowa z obrazka.

Średnio użytkownicy potrzebowali 10 spojrzeń na przeczytanie obrazka, a 50% badanych potrzebowała mniej niż 9 spojrzeń. Z prawdopodobieństwem 95% można stwierdzić, że liczba spojrzeń potrzebnych na przeczytanie obrazka w populacji zmieści się pomiędzy 7 a 13.

Średni łączny czas trwania spojrzeń wyniósł ponad 2 sekundy, a połowa badanych potrzebowała więcej niż 2,5 sekundy na wpisanie kodu. Z prawdopodobieństwem 95% można stwierdzić, że w populacji łączny czas potrzebny na przeczytanie obrazka nie przekroczy 3,1 sekundy.

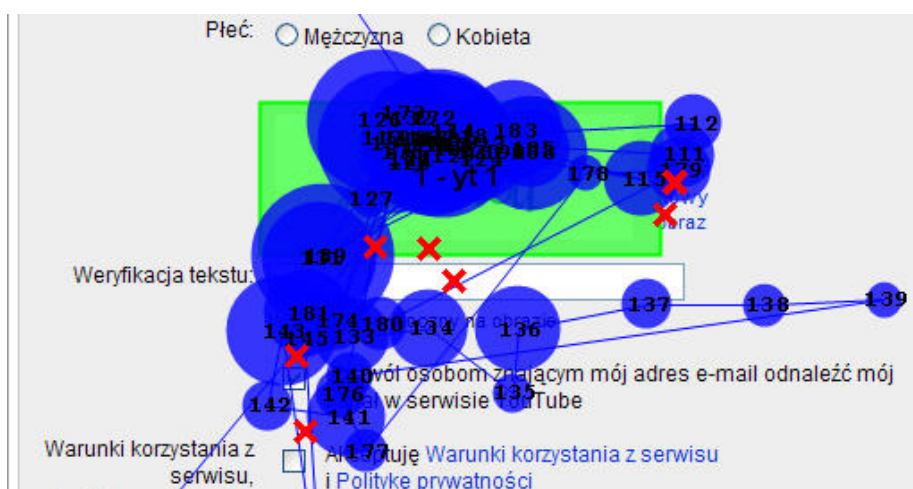
	Liczba fiksacji	Łączny czas trwania fiksacji w ms
Średnia	10	2393
Mediana	9	2553,5
Odchylenie standardowe	3,14	784,61
Wariancja próbki	9,84	615608,70
Kurtoza	-1,68	-0,60
Skośność	0,22	0,23
Minimum	6	1378
Maksimum	14	3709
Poziom ufności(95,0%)	3	656

Rysunek 22 Dane statystyczne dla liczby spojrzeń i łącznego czasu spojrzeń na kod CAPTCHA w serwisie Gazeta.pl

Konto serwisu Youtube.pl



Rysunek 23 CAPTCHA w serwisie Youtube



Rysunek 24 Gazeplot (ścieżki i czas spojrzeń) na kod CAPTCHA w serwisie Youtube.pl

Statystyka opisowa dla liczby fiksacji i łącznego czasu trwania fiksacji CAPTCHA zamieszczonego w serwisie Gazeta.pl wskazuje na umiarkowaną liczbę spojrzeń potrzebnych do wpisania słowa z obrazka.

Średnio użytkownicy potrzebowali 11,5 spojrzeń na przeczytanie obrazka, a aż 50% badanych potrzebowało więcej niż 13 spojrzeń. Z prawdopodobieństwem 95% można stwierdzić, że liczba spojrzeń potrzebnych na przeczytanie obrazka w populacji zmieści się pomiędzy 7,5 a 15,5. Średni łączny czas trwania spojrzeń wyniósł ponad 3,5 sekundy a połowa badanych potrzebowała więcej niż 3.2 sekundy na wpisanie kodu.

Z prawdopodobieństwem 95% można stwierdzić, że w populacji łączny czas potrzebny na przeczytanie obrazka nie przekroczy 5 sekund. Należy zwrócić uwagę, że w jednym przypadku osoba potrzebowała aż 20 spojrzeń, co znacznie zawyżyło średnią i zniekształciło miary skośności.

	<i>Liczba Fiksacji</i>	<i>Łączny czas trwania fiksacji</i>
Średnia	11,5	3527
Mediana	13	3232
Odchylenie standardowe	5,10	1630,32
Wariancja próbki	26	2657958,57
Kurtoza	-0,63	-2,17
Skośność	0,17	0,16
Minimum	5	1595
Maksimum	20	5643
Poziom ufności(95,0%)	4	1363

Rysunek 25 Dane statystyczne dla liczby spojrzeń i łącznego czasu spojrzeń na kod CAPTCHA w serwisie Youtube.pl

Porównanie średnich dla różnych serwisów

Celem porównania liczby fiksacji i łącznego czasu spojrzeń użytkowników na poszczególne grupy wykonano „test t dla średnich”, przyjmując hipotezę zerową, że średnie dla liczby spojrzeń i łącznego czasu spojrzeń na CAPTCHA w różnych serwisach są równe. Poniższe tabele zawierają wskaźnik „*p-value*” dla 95% przedziału ufności.

	o2	Gazeta	YouTube
o2	-	0,003	0,020
Gazeta	0,003	-	0,566
YouTube	0,020	0,566	-

Rysunek 26 Wskaźnik „p-value”.

W przypadku serwisu o2 wszystkie wskazania są poniżej 5%, co świadczy o tym, że hipotezę o równości średniej liczby spojrzeń należy odrzucić. CAPTCHA w serwisie o2 potrzebuje statystycznie mniej spojrzeń niż w pozostałych serwisach. W przypadku Gazety i YouTube można przyjąć, że średnia liczba spojrzeń potrzebnych na przeczytanie słowa z obrazka jest taka sama.

	o2	Gazeta	YouTube
o2	-	0,025	0,032
Gazeta	0,025	-	0,113
YouTube	0,032	0,113	-

Rysunek 27 Wskaźnik „p-value”.

W przypadku średniego łącznego czasu spojrzeń występują istotne statystycznie różnice pomiędzy wszystkimi serwisami. Najkrócej wpatrują się w kod użytkownicy w serwisie o2.pl, dłużej w Gazeta.pl, a najdłużej w YouTube.pl.

8. Podsumowanie

CAPTCHA zastosowane w serwisie o2.pl wymaga od użytkowników zdecydowanie najmniej wysiłku. Potrzebują oni niewiele krótkich spojrzeń, aby przeczytać i poprawnie wpisać kod. Liczba spojrzeń w serwisie Gazeta.pl i YouTube.pl jest zbliżona, ale w Gazeta.pl trwają one krócej, co oznacza, że użytkownicy mają mniejszy problem z przeczytaniem kodu.

Kod weryfikacyjny w serwisie Youtube.pl, mimo, że najtrudniejszy do odczytania, jest równocześnie najtrudniejszy do złamania przez oprogramowanie OCR. Stłoczone znaki, utrudniają przeczytanie i prawidłowe wpisanie kodu, zarówno użytkownikowi, jak i botowi.

Youtube.pl wprowadzając opcję odśwież, znalazł złoty środek, między użytecznością kodu, a bezpieczeństwem. Liczba fiksacji została w badaniu ograniczona do fiksacji efektywnych, czyli, tych spojrzeń, które doprowadziły do wpisania kodu z obrazka. Możliwość odświeżenia kodu i przeskakiwania przez kolejne generowane CAPTCHA w serwisie Youtube, wpływa na wydłużenie czasu potrzebnego do wpisania kodu.

Kolejna kwestia to problem związany z widocznością przycisku odświeżającego dla użytkownika w serwisie Youtube.pl. Brak informacji czym jest przycisk „nowy obrazek” wpływa dodatkowo na wydłużenie czasu potrzebnego na wpisanie kodu w przypadku osoby, która ma problem z jego odczytaniem i nie korzysta z opcji odświeżenia (nie wnikając dlaczego nie korzysta).

Badane serwisy w przypadku nieprawidłowego wpisania CAPTCHA nie karzą użytkownika koniecznością przechodzenia raz jeszcze poprzez wszystkie pola formularza. Do poprawy jest tylko kod weryfikacyjny, błędnie wypełnione pole, ewentualnie powtórzenie hasła jak w Youtube.pl.

Odświeżanie całego formularza i utrata danych w przypadku nieprawidłowego wpisania kodu, kiedyś stanowiły jeden z większych powodów do frustracji dla użytkowników.

Reasumując wyniki badań, własne spostrzeżenia i wypowiedzi ekspertów, możemy określić, czym powinno się charakteryzować dobre CAPTCHA:

- dobre CAPTCHA to takie, które zapewnia bezpieczeństwo serwisu i nie jest jednocześnie utrapieniem dla użytkowników,
- powinno zapewniać dostęp do serwisu użytkownikom niepełnosprawnym,
- powinno zawierać przycisk odśwież,

- powinno informować o ilości koniecznych do wpisania elementów,
- powinno odzwierciedlać specyfikę kulturową,
- powinno zawierać informacje dlaczego należy je wpisać,
- powinno dawać możliwość dodatkowej np. telefonicznej weryfikacji użytkownika,
- powinno podlegać czasowym ewaluacjom bezpieczeństwa.

Należy jednak nadmienić, że nie w każdym przypadku wszystkie wyżej wymienione elementy mają zastosowanie w pojedynczym kodzie CAPTCHA.

9. Kilka słów o Symetrii

Symetria od 1998 roku specjalizuje się w planowaniu i kompleksowej obsłudze projektów związanych z szeroko pojętym e-commerce. Firma ma tym polu bardzo duże osiągnięcia, poparte wymiernymi sukcesami.

Doświadczenie Symetrii, kompetencje oraz szerokie kontakty z największymi polskimi firmami internetowymi gwarantują profesjonalizm i kompleksowość dostarczanych rozwiązań.

Z naszych usług korzystają największe firmy, m.in.:



Więcej na temat użyteczności oraz badań z użytkownikami dowiesz się na stronie [Symetrii](#) oraz na [blogu](#).

Agencja e-biznes Symetria udostępnia na swoich stronach internetowych darmowe publikacje z zakresu użyteczności, badań eye trackingowych oraz e-marketingu. Każdy zainteresowany użytkownik może pobrać na swój dysk interesującą go publikację w naszym dziale:

http://www.symetria.pl/html/i_44_ogolem.html



Rysunek 28 Dwa górne print screeny przedstawiają stronę Symetrii dwa dolne symetrycznego bloga.