MASARYKOVA UNIVERZITA
FAKULTA INFORMATIKY


# CAPTCHA – automatizovaný Turingov test

BAKALÁRSKA PRÁCA

**Róbert Bariak**

Brno, jar 2013

# Prehlásenie

Prehlasujem, že táto bakalárska práca je mojím pôvodným autorským dielom, ktoré som vypracoval samostatne. Všetky zdroje, pramene a literatúru, ktoré som pri vypracovaní používal alebo z nich čerpal, v práci riadne citujem s uvedením úplného odkazu na príslušný zdroj.

Róbert Bariak

Vedúci práce: RNDr. Marek Kumpošt, Ph.D.

# Poďakovanie

Chcel by som poďakovať RNDr. Marekovi Kumpoštovi, Ph.D. za pomoc pri písaní práce a taktiež rodine za podporu.

# Zhrnutie

Táto práca sa zaoberá technológiou Captcha. Cieľom je oboznámiť čitateľa s dôvodmi pre vznik Captcha, s rôznymi druhmi, útokmi a pokúsime sa objasniť, ako sa priblížiť ku ideálnej Captcha

Praktická časť práce sa venuje programovaniu Captcha, výstupom je funkčná Captcha založená na rozpoznávaní textu.

## Kľúčové slová

captcha, umelá inteligencia, bot, spam, Turingov test, OCR

# Obsah

# Úvod

Spam už dávno nie je iba doménou e-mailových správ, ale aj rôznych webových služieb, ktoré umožňujú užívateľom vkladať akýkoľvek obsah alebo registrovať sa k nim. Vo väčšine prípadov sú za tento spam zodpovední roboti. Spam však zďaleka nie je to najhoršie, čo títo roboti dokážu. Ich rôzne automatizované útoky majú horšie následky ako útoky jednotlivca a práve preto sa tento problém dá, zjednodušene povedané, zúžiť na problém rozoznania ľudí od robotov. O to sa snaží technológia Captcha, o ktorej je táto bakalárska práca. Cieľom bakalárskej práce je zhrnúť najdôležitejšie fakty o tejto technológii, používanej od roku 2000. Kým druhá kapitola vysvetľuje a objasňuje dôvody jej vzniku, tretia kapitola popisuje najrôznejšie bežne využívané typy Captcha, s ktorými sa pri potulkách internetom môže užívateľ stretnúť. V štvrtej kapitole sú popísané niektoré z útokov na systémy Captcha a piata sa venuje ideálnej Captcha, jej vlastnostiam a hodnoteniu súčasných Captcha testov podľa týchto vlastností. Šiesta kapitola popisuje praktickú časť práce.


**Obr. 1.1**: *Budúcnosť Captcha?*

**Prevzatý z [11].**

# Kapitola 2

## Automatizovaný Turingov test

Vznik Captcha reflektuje potrebu brániť sa proti zneužívaniu webových služieb, ako proti množiacim sa robotom, ktorí spamujú diskusie a chaty komerčnými propagáciami a zakladajú tisícky e-mailových kont (na stránkach spoločností Google, Yahoo a Hotmail [1]), z ktorých následne rozosielajú spam[1] – napríklad reklamu v masovom meradle. Okrem toho sa stretávame s pokusmi o manipulácie s online hlasovacími systémami, ničenie integrity webových stránok, prístup k súkromným informáciám alebo šírenie škodlivého kódu. Všetky tieto snahy vedú k ziskovej činnosti samotných spamerov a trápia majiteľov stránok a tí radi siahajú na riešenie pomocou Captcha. Captcha teda reaguje na reálne problémy na webe. Iba projekt ReCaptcha od Google odhaduje, že denne je vyplnených viac ako 200 miliónov Captcha testov, pričom vyplnenie jedného trvá približne 10 sekúnd. Existujú však aj argumenty proti použitiu Captcha, napríklad Tim Kadlec tvrdí, že: „*...spam nie je problémom užívateľa, je problémom firmy prevádzkujúcej webovú stránku. Je arogantné a lenivé snažiť sa presunúť problém na návštevníkov stránok.*“ [2]. Používanie predovšetkým najznámejšej varianty na rozpoznávanie a prepísanie textu je však dnes už štandardom na weboch ako Google, Facebook alebo eBay. Je dôležité pripomenúť, že cieľom Captcha nie je úplne vylúčiť rôzne útoky, ale ich do značnej miery obmedziť a poskytnúť pred nimi istý stupeň ochrany.

## 2.1 Turingov test

Captcha znamená ***C****ompletely* ***A****utomated* ***P****ublic* ***T****uring test to tell* ***C****omputers and* ***H****umans* ***A****part*, teda plnoautomatizovaný verejný Turingov test na rozlíšenie počítačov a ľudí. Ako názov napovedá, je Captcha podobná *Turingovmu testu*, ktorý v roku 1950 predstavil anglický matematik Alan M. Turing [22]. Ten pozostáva z dvoch hlavných

[1] **spam** je nevyžiadaná a hromadne rozosielaná správa prakticky rovnakého obsahu. Ide o zneužívanie elektronickej komunikácie, najmä e-mailu. Zdroj: Wikipedia

aktérov – človeka a počítača, pričom obaja sa snažia test presvedčiť, že sú človek, a rozhodcu, ktorý bez toho, aby ich videl, im kladie otázky. Entita spĺňa Turingov test vtedy, ak rozhodca nevie rozoznať, či komunikuje s človekom alebo počítačom. Zaujímavosťou je, že sa doposiaľ ešte žiadnemu stroju nepodarilo na 100% prejsť Turingovym testom.

## 2.2 Captcha

Captcha je test, ktorý má byť pre človeka čo najjednoduchší a zároveň ho nedokáže vyriešiť súčasný počítačový program. Captcha vychádza práve z Turingovho testu, avšak rozhodcom nie je človek, ale počítač – ako napovedá „*completely automated*". Prvoradou úlohou je odlíšiť ľudských užívateľov od automatických skriptov a internetových robotov. Formálna definícia je k dispozícií v článku [3]. Captcha úzko súvisí s umelou inteligenciou. S tým, ako sa postupne umelá inteligencia vyvíja, je potrebné vylepšovať aj Captcha testy.

Prvým, kto navrhol použiť automatizované Turingove testy na overenie, že na druhej starne nečíha bot[2], bol v roku 1996 izraelský profesor Moni Naor [10] . Už o rok neskôr sa Captcha test objavuje na vyhľadávači Alta-Vista pri pridávaní URL adries, ako reakcia na množiace sa útoky a snahu manipulovať s poradím vyhľadávaných stránok [3]. Samotný názov Captcha bol ale prvýkrát použitý až v roku 2000 tímom na Carnegie Mellon University, ktorý sa významnou mierou pričinil o popularitu tejto technológie. Tento tím vytvoril tzv. Gimpy Captcha [5], kde boli zachytené náhodné slová, ktoré boli deformované a prekryté rôznymi tvarmi, ktoré mali sťažiť prehľadnosť pre programy na rozoznávanie textu. Práve táto obrázková Gimpy Captcha, v zjednodušenej forme, kde užívateľ zadáva jediné slovo a nie hneď niekoľko, sa stala a pretrvala synonymom boja proti nechceným botom. Vysvetlili tiež druhý význam názvu Captcha, a to ***CAPT****ure* ***CHA****racters* – prečítaj znaky. V priebehu času sa však vyrojili a aj zdokonalili rôzne automatizované útoky na technológie Captcha.

[2] **bot** -počítačový program, ktorý pre svojho majiteľa opakovane vykonáva nejakú rutinnú činnosť na internete.

Najčastejšie sa Captcha uplatňuje v nasledovných oblastiach:

- **Vyhľadávací roboti** (*search engine bots*) – Captcha dokáže týmto robotom zabrániť čítať internetové stránky použitím html tagu, takže je robotom neprístupná.
- **Ochrana e-mailových adries pred *web scrapingom***[3] – schopná Captcha dokáže skryť e-mailové adresy pred scrapermi, takže užívateľ predtým, ako mu je sprístupnená e-mailová adresa, musí úspešne vyriešiť Captcha, čo sa zdá ako perfektné riešenie problému web scrapingu.
- **Ochrana registrácie na weboch** – Captcha sa bežne využíva na ochranu služieb poskytovateľov bezplatných e-mailových adries. U týchto spoločností (napr. Gmail, Microsoft, Yahoo) si užívateľ môže zaregistrovať jedno alebo viacero e-mailových kont, v dôsledku čoho útočníci môžu registrovať (za pomoci určitých programov) tisíce kont za minútu. Captcha pomáha zamedziť tomuto trendu.
- **Červy**[4] **a spam** – Captcha sa ukazuje ako účinné riešenie proti červom a spamu.
- **Online hlasovania** – od vzniku internetu sa online hlasovania stali veľmi populárne. V roku 1999 istá internetová stránka spustila online hlasovanie o najlepšiu školu so zameraním na počítačové vedy. Keďže vedeli, že každý užívateľ môže hlasovať viac než raz, chceli tomu zabrániť pomocou zapamätania IP adresy užívateľa. Potom však dve školy našli spôsob použitím programu, s ktorým mohli hlasovať neobmedzene. Aj tu sa Captcha javí ako vhodná ochrana pred automatizovaným hlasovaním. [4]

[3] **web scraping** - softwarová techniku získavania informácií z webových stránok. Web scraping má blízko k webovému indexovaniu, kde robot indexuje obsah webových stránok a ktoré využíva väčšina internetových vyhľadávačov. Zdroj: http://4it417.blogspot.cz/2010/12/web-scraping.html

[4] **červ** je program so škodlivým kódom, ktorý napáda hostiteľský počítač, využíva jeho prepojenie cez sieť s ďalšími počítačmi a prostredníctvom nich sa šíri ďalej. Zdroj: Wikipedia

# Kapitola 3

# Typy captcha

Zatiaľ čo druhá kapitola mala za úlohu popísať, k čomu Captcha slúži, tretia predstaví najbežnejšie používané druhy Captcha. Každý typ môže mať ešte množstvo variácií, tým sa však venovať nebudeme, keďže sa väčšinou líšia len v nie príliš významných detailoch. Rovnako sa táto kapitola samostatne nevenuje zvukovej Captcha, pretože v praxi je najviac využívaná ako doplnková alternatíva k iným typom Captcha, určená pre handicapovaných ľudí. Verím, že vybrané typy dostatočne pokryjú najvýznamnejšie používané implementácie.

## 3.1 Captcha založená na rozpoznávaní textu

Hoci od vytvorenia prvej Captcha prešlo relatívne veľa rokov a v dnešnej dobe existujú stovky rôznych dizajnových variácií, stále prevažujú tie, ktoré sú založené na texte (originálny názov angl. *text based*). Hlavným dôvodom je, že ich implementácia aj dizajn sú jednoduché [1]. Typicky táto Captcha funguje tak, že generuje statický obrázok, v ktorom sa v popredí nachádza skupina znakov a úlohou testovaného je bezchybne prepísať znaky do pripraveného formulára. Aby to nebolo príliš triviálne, obvykle má túto úlohu sťažiť deformácia textu o určený uhol, uloženie písmen veľmi blízko pri sebe alebo až v sebe a pozadie, ktoré častokrát obsahuje ďalšie znaky - prípadne len čiary alebo iné tvary - sčasti prekrývajúce text v popredí. Captcha založená na rozpoznávaní textu je tak hojne využívaná, že keď človek pri odosielaní nejakého príspevku vo fóre, registrácii alebo inej činnosti vidí skupinu zdeformovaných znakov, už dopredu vie, že jeho úlohou je prepísať ich.

Už vyššie spomínaná *Gimpy Captcha* [23], pôvodne vyvíjaná pre a s Yahoo, zachytávala náhodné anglické slová, tie ukladala ako obrázok s tlačeným textom, ktorý bol rozlične deformovaný a prekrytý inými znakmi alebo tvarmi. Predpokladá, že človek dokáže na rozdiel od technológie OCR[5], ktorý je využívaná botmi pri snahe prekonať tento druh Captcha testu, prečítať aj defektný text. Užívateľovi zobrazila isté

[5] **Optical Character Recognition** – optické rozoznávanie znakov, technológia na získanie textu z obrázku

množstvo slov a on mal určitú časť z nich správne prepísať, aby úspešne prešiel testom. Zjednodušená *EZ Gimpy Captcha* už ponúka len jediné slovo. Bežná Captcha, založená na rozpoznávaní textu však nutne neponúka platné slovo zo slovníka, ale len kombináciu znakov a (alebo) číslic. Pri dĺžke slova 5 znakov a 36 rôznych znakoch a číslic je k dispozícii zhruba 60 miliónov rôznych variácií. Rôzne obmeny môžu zahŕňať aj zmenu pozadia, ktoré by nemalo byť statické a rovnaké pre všetky vygenerované Captcha.

Nanešťastie platí, že čím náročnejšie je rozoznanie textu pre počítač, tým väčšie ťažkosti s ňou má aj človek. Preto neprimerané deformácie môžu spôsobiť, že ani človek neprejde testom, prípadne niektoré znaky budú pripomínať viac písmen. Najčastejšie takéto prípady uvádza Tabuľka 1.

| Pôvodný znak | Môže sa javiť ako | Pôvodný znak | Môže sa javiť ako |
|---|---|---|---|
| **vv** | w | ln | h |
| **cl** | d | ob | do |
| **rn** | m | op | qo |
| **rm** | nn | wv | vw |
| **nn** | m | vw | wv |
| **cm** | an | NV | W |
| **bl** | lol alebo ld | LH | 44 |
| **bp** | lop | FNN | AW |
| **ld** | lol alebo bl | VV | W |
| **do** | ob | | |

**Tabuľka 1 – Chyby v rozoznávaní textu. Prebraté z: [7].**

V roku 2007 bol vytvorený projekt reCAPTCHA, ktorý patrí dnes medzi najpopulárnejšie. Využíva ho napríklad aj Google, ktorý ho odkúpil v roku 2009, tiež ho poskytuje bezplatne k stiahnutiu na vlastné webové stránky. Inakosť tohto projektu spočíva v tom, že reCaptcha pomáha digitalizovať staré vydania New York Times a knihy z Google Books a že sú užívateľovi ponúknuté hneď dve slová. Jedno slovo slúži, tak ako pri iných Captcha testoch, na rozlíšenie robota od človeka. Toto slovo sa nazýva *kontrolné*. Je to zdigitalizované slovo, ktoré bolo jednoznačne identifikované a teda označené za vyriešené. Druhé slovo je slovo, ktoré technológia OCR pri skenovaní nedokázala rozpoznať. Každý, kto už skúšal skenovať text pomocou tejto technológie priamo do textového editora, sa s niektorými jej nedostatkami už určite stretol. Predovšetkým pri starších dielach sa nedarí rozpoznať množstvo slov.

ReCaptcha predpokladá, že každý, kto úspešne rozlúštil kontrolné slovo, prepísal úspešne aj druhé slovo. To v praxi znamená, že každý takýto užívateľ pomáha pri digitalizácii kníh. Aby sa zamedzilo špekuláciám, že užívateľ vyplní len kontrolné slovo a druhému sa vyhne, nie je poradie kontrolného slova pevné. Taktiež nestačí, aby slovo prepísané jediným užívateľom bolo považované automaticky za správne. Až keď nastane zhoda u dostatočného počtu pokusov, použije sa prepis pri digitalizácii.

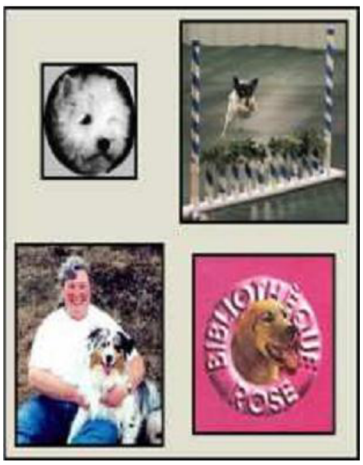

**Obr. 3.1: reCaptcha. Prevzatý z Google.**

Ako vidieť aj na Obr. 3.1, táto technológia obsahuje jeden veľmi dôležitý prvok, a to možnosť refreshu (obnovenia) ponúknutých slov. Mnohokrát práve táto chýbajúca funkcia dokáže zahatať človeku úspešný priechod Captcha testom. Okrem toho myslí aj na ľudí so sluchovou vadou, preto obsahuje alternatívu hovoreného slova. Je prečítaných 8 čísel, ktoré užívateľ prepíše pomocou klávesnice. Táto alternatíva, rovnako ako pri písanom texte, nesmie byť príliš triviálna, pretože ani vlastnosti technológie rozoznávania reči sa v zásade nelíšia od rozoznávania textu OCR. Existujú programy, ktoré zvuk rozdelia na jednotlivé hlásky, ktoré potom vie jednoducho previesť na text. A napokon rovnako ako pri OCR, je najdôležitejší optimálny pomer medzi deformáciou a rozpoznateľnosťou, v opačnom prípade sa stane, že nebude plniť svoj účel. Faktom ale ostáva, že aj vďaka rozšírenosti tohto typu Captcha sa boti, pred ktorými nás má chrániť, tiež zlepšujú vo využívaní technológie OCR.

## 3.2 Obrázková Captcha

Práve Capcha test, ktorý je založený na vizuálnom rozpoznávaní objektov na obrázkoch (prípadne orientácie obrázku alebo iné), má byť alternatívou, ktorá je voči tejto technológii odolná. Ďalšie plus má byť, že na rozdiel od spomínaného typu sa esteticky viac hodí do webového prostredia a nepôsobí natoľko rušivo.

Jednou z prvých technológií bola PIX-Captcha [4]. Táto pozostáva zo súboru kreslených obrázkov alebo (a) fotiek, ktoré znázorňujú spoločný objekt (napríklad dom, strom, psa), ktorý je pre človeka čo možno najjednoduchšie rozpoznateľný. Dôležité je aj to, aby bol jednoznačne identifikovateľný, to napríklad znamená, že daný objekt nebude mať niekoľko synonymických názvov.




**Obr. 3.2: Príklad PIX-Captcha. Objektom je pes [4].**

Užívateľovi je teda predložený súbor niekoľkých obrázkov (v prípade príkladu na Obr.3.2 sú to 4) konkrétneho objektu a jeho úlohou je určiť názov objektu. Podľa implementácie potom závisí, či užívateľ tento názov vyberie z ponúkaných možností alebo ho sám naťuká do formulára. Hlavnou nevýhodou, ktorá zrejme aj spôsobila, že tento typ sa masovo neujal je fakt, že databáza obrázkov a objektov je primalá.

Ako ďalší príklad uvediem bezplatne dostupnú technológiu Asirra[6] od firmy Microsoft, ktorá spĺňa intuitívnu definíciu Captcha z úvodnej kapitoly – Asirra, ktorá ponúka 12 snímok zvierat (psov a mačiek) a kladie užívateľovi za úlohu označiť všetky mačky, je jednoduchý test, ktorý zvládne zrejme aj dieťa škôlkarského veku, no pre počítač to nie je triviálna úloha. Výskum Microsoftu uvádza, že úspešnosť riešenia je v intervale do 30 sekúnd až 99,6% [5].

Tiež sa dá predpokladať, že mačky sú od psov vždy ľahko rozlíšiteľné, na rozdiel od niektorých deformovaných znakov pri niektorých implementáciách Captcha založenej na rozpoznávaní textu. Je nutné pripomenúť, že nápad využiť snímky zvierat nie

[6] **Animal Species Image Recognition for Restricting Access** – rozoznávanie zvierat na obrázku pre zabránenie prístupu

je pôvodný, boli tu už projekty ako KittenAuth[7], ale Asirra rieši základný problém svojich predchodcov, a to veľmi malú databázu, z ktorej obrázky čerpá. Nie je totiž problém spustiť test niekoľkokrát, zrekonštruovať celú databázu a realizovať útok. Pri


**Obr. 3.3: Úspešné zložený Captcha test Asirra.**

**Prevzaté z http://www.sg.hu/**

Asirre to však bude zložitejšie, pretože jej databáza je dynamická a prakticky nekonečná – jedná sa totiž o databázu odchytených túlavých zvierat, ktorým sa hľadá nový domov prostredníctvom webu Petfinder.com.

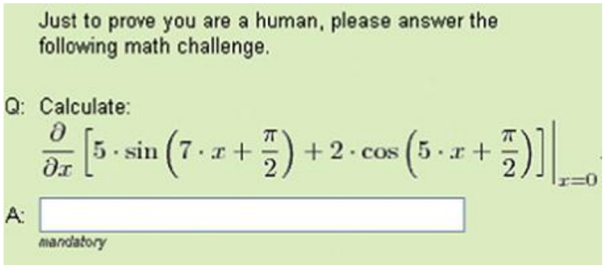
## 3.3 Matematická Captcha

Tento druh patrí medzi tie s najvyššou užívateľskou úspešnosťou pri riešení. V roku 2012 sa v Nemecku uskutočnil prieskum, zverejnený v [8]. Jeho predmetom bola okrem iného aj úspešnosť riešenia Captcha systémov. Zúčastnilo sa ho 50 testovaných osôb, rozdelených do skupín študenti a ostatní, a zo vzorky 150 jednotlivých pozorovaní na každú variantu Captcha, bola celková úspešnosť (bez ohľadu na skupinu) tej matematickej až 98,67%, pričom napríklad spomínaná Asirra dosiahla úspešnosť prekvapivo „iba“ 84%. Pre použitie matematickej varianty Captcha hovorí aj druhý výstup tohto prieskumu. Podľa neho je priemerný čas, potrebný na úspešné vyriešenie iba 7,27 sekundy, čo z nej robí najvýhodnejšiu variantu. Bližšie výsledky tohto

[7] **Kittenauth.com** – ponúka 12 obrázkov rôznych zvierat a užívateľ musí označiť všetky mačky, aby zdolal test. Táto technológia pracuje so statickou databázou.

prieskumu sú uvedené v 4. kapitole. Na druhej strane však jednoduchá matematická Captcha podlieha skenovaniu technológiou OCR rovnako dobre, ako typické Captcha testy založené na rozpoznávaní textu. Zjednodušene povedané, technológia OCR načíta jednotlivé znaky – čísla a operátory, program rovnicu vypočíta a výstupom je výsledok. Bežné matematické Captcha sa totiž skladajú z dvoch jednociferných, maximálne dvojciferných čísel a obsahujú jeden zo základných matematických operátorov (+, -, x, /). Riešením, ako to technológii OCR naozaj skomplikovať, je používanie aj zložitejších matematických symbolov. Otázkou však je, či taká náročná Captcha plní svoj pôvodný účel, a to že má byť jednoduchá pre človeka.

Príkladom takej technológie je matematická Captcha[8] chorvátskeho Ruder Boškovic Institute. Ich služba je ponúkaná po registrácii bezplatne a vyžaduje pokročilú úroveň matematických schopností. Systém sa spolieha na svoj samostatný hardwarový generátor čísel. Stránka náhodne ponúkne jeden z matematických problémov, ktoré má užívateľ vyriešiť.




**Obr. 3.4: QRBGS Captcha. Prevzaté z [5].**

Ponúka, našťastie, aj jednoduchšie úlohy, ktoré sú založené len na základných operátoroch, avšak úlohy sú zložitejšie, keďže namiesto dvoch výrazov ich obsahujú niekoľkonásobne viac. Zvyšuje sa tým najmä časová náročnosť na vyriešenie úlohy, preto táto implementácia nie je práve najšťastnejšou. Captcha je už beztak vnímaná bežným užívateľom ako otravná súčasť internetu. Užívateľ má síce možnosť refreshu, pričom dostane nový test, ktorý môže byť menej náročný, no aj táto možnosť je neefektívna a zdržujúca. Aj sami autori totiž tvrdia, že jej vyriešením nielenže potvrdíte, že ste človek, ale že ste človek dostatočne dobrý v matematike.

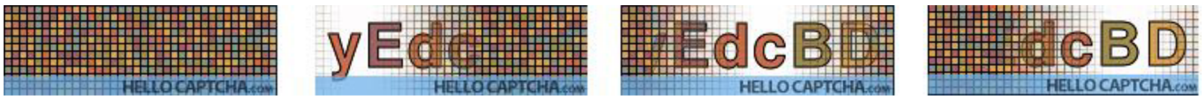
[8] Captcha má názov „Quantum Random Bit Generator Service“ a je dostupná na http://random.irb.hr/

## 3.4 Animované (video) Captcha

Hoci tento druh Captcha nepatrí medzi najpoužívanejšie, je rozhodne zaujímavý a inovatívny. Táto kategória zahŕňa testy, ktoré sú tvorené flash[9] animáciou, animovaným obrázkom formátu GIF, alebo streamom[10] videa.

Asi najznámejším zástupcom je *NuCaptcha* [24]. Technológia samú seba nazýva ako „Human friendly" Captcha, čiže priateľskú k ľuďom. Jej podstatou je prepísať červené znaky z textu v popredí, letiaceho sprava doľava. Text pôsobí, ako by sa vnášal na vlnách. Tri červené znaky sa nachádzajú na konci správy, čo však nie je problém, pretože pri načítaní text nezačne prichádzať od prvého znaku, ale už „ubehol" náhodnú dráhu. NuCaptcha ponúka na výber niekoľko tém pozadia, ktoré sú spravidla tiež animované a majú zabezpečiť väčšiu homogénnosť animácie. Narozdiel od všetkých doteraz popisovaných Captcha testov, je NuCaptcha komerčný produkt s možnosťou vyskúšania 30-dňovej trial verzie.

Ako bezplatnú alternatívu spomeniem *HelloCaptcha* [26], ktorá ponúka až 12 rôznych variant animovaných testov, pričom všetky sa dajú prezrieť a vyskúšať na oficiálnej webovej stránke. Jedná sa o animované obrázky typu GIF s veľkosťou 180x60 pixelov a šiestimi znakmi a (alebo) číslicami. Ako tvorcovia sami tvrdia, ich captcha je odolná voči botom, pretože animácia pridáva ďalšiu dimenziu (čas) do útočníkovho algoritmu. Ako však uvádza dokument [12], niektoré typy nie sú odolné voči útoku segmentáciou – oddelením znakov a následne rozpoznávaním každého znaku samostatne. Popísali rôzne metódy, ako účinne prelomiť všetky typy HelloCaptha a ukazuje, že hoci čas ako ďalšia dimenzia zvyšuje odolnosť testu, ak nie je navrhnutá dostatočne dobre, míňa sa svojmu zámeru.




**Obr. 3.5: Príklad HelloCaptcha – varianta SpreadFade v 4 sekvenciách. Prevzaté z: [26].**

[9] **Flash animácia** - animácia, ktorá využíva vektorovú grafiku. Je určená na prehliadanie, nie je vhodná na ďalšie použitie. Môže byť obohatené o zvuk a interaktivitu (návštevník môže zasahovať do priebehu animácie). Prevzaté z: http://di.ics.upjs.sk/informatika_na_zs_ss/studijny_material/grafika/flash/co_je_flash.htm

[10] **streaming** znamená priebežný prenos bez nutnosti ukladať celý súbor (alebo jeho väčšie úseky) na strane užívateľa. Umožňuje prehrávanie audia a videa veľmi krátko po nadviazaní spojenia so serverom. Prevzaté z: http://standardy.informatika.sk/node/28

## 3.5 Puzzle Captcha

Zaujímavou formou Captcha testu je tzv. *Jigsaw puzzle Captcha* [13], teda skladačka. Užívateľovi je predložený obrázok, rozdelený do *n*x*n* obdĺžnikov, pričom dve z nich sa nachádzajú na nesprávnom mieste, a užívateľ ich musí vymeniť. Použité obrázky musia byť dôkladne vyberané, pretože pri ich rozrezaní môže vzniknúť taký obdĺžnik, pri ktorom užívateľ len ťažko určí, či nepatria na iné miesto.

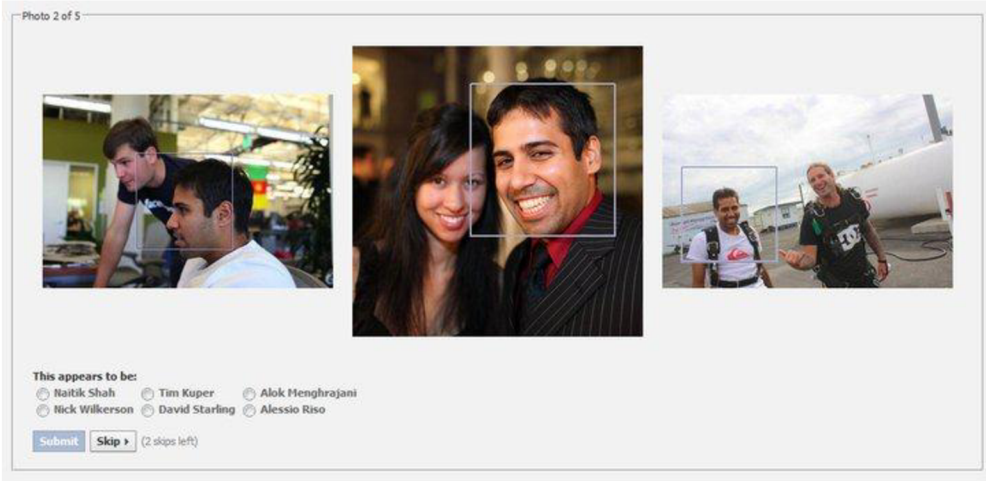
Obrázky pochádzajú z internetu, prevažne z vyhľadávania Google a sú vyberané náhodne a až následne triedené na vhodné a nevhodné. Vytriedené obrázky prechádzajú testovaním na vzorke 100 užívateľov, cez ktoré prejdú len tie s úspešnosťou riešenia nad 60%. Autori venovali pozornosť aj hranám jednotlivých obdĺžnikov, z ktorých je obrázok poskladaný. Pozdĺž každej hrany sú body zafarbené na bielo, a to náhodne do hĺbky medzi 5-10 bodov. Pri všetkých troch veľkostných variantoch (3x3, 4x4, 5x5) sa úspešnosť riešenia pohybuje od 87,6% (pri 5x5) do 89% (pri rozmere 3x3). Jedná sa určite o zaujímavý Captcha test.


**Obr. 3.6: Puzzle Captcha. Prevzaté z [13].**

## 3.6 Rozpoznávanie priateľov

So zaujímavým nápadom prišiel v roku 2011 Facebook, ktorý postupne začína tradičnú – textovú Captcha, nahrádzať ich tzv. *sociálnou autentifikáciou*. To znamená, že užívateľovi sa zobrazí niekoľko fotiek, na ktorých sa nachádzajú jeho priatelia na tejto sociálnej sieti a on má rozhodnúť, o koho sa jedná. Užívateľ má rozoznať celkom 5 svojich priateľov, každého z nich uvidí na 3 fotografiách. Vybrať musí zo 6 ponúknutých mien. Keďže sa nezobrazujú len fotografie priamo z profilu daných ľudí, ale ľubovoľné fotky, na ktorých majú menovku, má byť šanca, že útočník identifikuje všetkých 5 osôb, minimálna. Ako tvrdia autori, táto metóda má ambíciu vytlačiť

klasickú Captcha z Facebooku, pretože *„hackeri môžu poznať Vaše heslo, ale nepoznajú Vašich priateľov.“* Tento variant je zatiaľ stále v testovaní, využíva sa pri účtoch, na ktorých bola zaznamenaná potenciálne nebezpečná aktivita, to znamená napr. viacnásobné prístupy z odlišných krajín v krátkych časových intervaloch alebo pokusy o súbežné prihlásenie z viacerých IP adries [14].




**Obr. 3.7: Sociálna autentifikácia. Prevzaté z [14].**

## 3.7 Reklamná Captcha

Príkladom tohto druhu je nemecká *CaptchaAd* [27], ktorá vznikla v roku 2008, kedy jej autori prišli s nápadom skombinovať pre nich otravnú, klasickú Captchu s reklamou. Užívateľovi je prehratý spravidla 15 sekúnd dlhý reklamný spot. Hneď po začiatku sa užívateľovi zobrazí otázka k obsahu alebo značke z reklamy, na ktorú dokáže na základe informácií z reklamy jednoznačne odpovedať – tak deklarujú autori. Po kliknutí na reklamu sa užívateľ dostane na webovú stránku produktu. CaptchaAd má byť v ideálnom prípade integrovaný do procesov, v ktorých je užívateľ zvyknutý na interakciu. Interakcia užívateľa s reklamou údajne vykazuje vysoký marketingový vplyv. Na obrázku 3.8 sa nachádza Captcha s reklamou na online lekáreň. Užívateľovi je položená otázka, v ktorej online-lekárni môže ušetriť až do 50%. Očakávaná odpoveď je názov lekárne z reklamy. Tento typ Captcha nepatrí k príliš využívaným, osobne ho však považujem za zaujímavý.


Obr. 3.8: CaptchaAd. Prevzaté z www.captchaad.de

# Kapitola 4

## Útoky na Captcha systémy

Captcha bola vyvinutá ako prostriedok, ktorý má zamedziť útočníkom v rozšírení automatizovaných útokov. Od jej vzniku až po súčasnosť sme svedkami neustáleho boja medzi autormi Captcha, ktorí sú nutení neustále vylepšovať túto technológiu a útočníkmi, ktorých cieľom je ovládnuť a prelomiť ju. Táto kapitola popisuje najbežnejšie útoky.

## 4.1 Útok opakovaním

*Útok opakovaním* (replay attack) spočíva v odpočúvaní časti komunikácie medzi dvoma autentizujúcimi stranami a následnom použití zachytených dát pri neskoršej autentizácii útočníka. Vyriešenie Captcha sa dá rozdeliť do minimálne troch krokov – odoslanie problému, odoslanie riešenia a nakoniec sa pošle odpoveď. Ak po úspešnom vyriešení Captcha systém danú reláciu (konkrétnu inštanciu Captcha) neukončí, je možné vykonať útok opakovaním. Nemusí byť ani prelomená daná Captcha, stačí, ak je raz vyriešená a robot opakovane použije danú odpoveď, pretože relácia je stále platná. Hoci tento útok teda vyžaduje ľudskú intervenciu (prvé vyriešenie Captcha), v prípade, že je čas do vypršania relácie dostatočne dlhý, je tento typ v praxi použiteľný a dobre škálovateľný. [25]

## 4.2 Útok segmentáciou

Tento typ útoku je hojne využívaný proti Captcha založených na rozpoznávaní textu. Cieľom segmentácie je rozdeliť obraz na disjunktné oblasti alebo na časti, ktoré sú homogénne z hľadiska vybranej vlastnosti, napríklad jasu, farby, odrazivosti, textúry apod. Pri tomto type útoku zvyčajne dochádza v prvom rade ku konverzii Captcha do čierno-bielej podoby, potom následne dochádza ku vertikálnej segmentácii (rozdeľovaniu) na niekoľko častí, pričom každá môže obsahovať jeden alebo viac znakov. Vertikálna segmentácia zahŕňa mapovanie obrázku do histogramu, ktorý

reprezentuje počet pixelov v jednotlivých blokoch na popredí obrázku a následne rozdelenie na kusy v miestach, ktoré neobsahujú žiadne pixely v popredí.

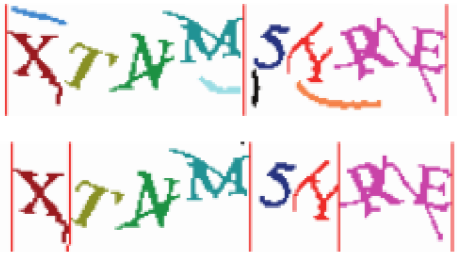
**Obr. 4.1: Vygenerovaná inštancia Captcha. Prevzaté z [28].**

**Obr. 4.2: Čierno-biela varianta a vertikálna segmentácia s histogramom. Prevzaté z [28].**

Na obrázku vidíme inštanciu Captcha rozdelenú na 2 kusy.

**Obr. 4.3: Captcha: Stav po vertikálnej segmentácii. Prevzaté z [28].**

V ďalšom kroku je aplikovaná segmentácia podľa farebnej výplne (CFS – color-filling segmentation) na oba kusy obrázku, čo zabezpečí identifikáciu všetkých spojitých častí resp. objektov, čo môžu byť znaky, línie, spojené línie alebo spojené znaky. Pri poznaní relatívnych pozícií objektov v týchto kusoch je možné s pomerne vysokou úspešnosťou rozlíšiť medzi skutočnými znakmi a rušivými líniami a krivkami. Častokrát sú línie sústredené najmä pri vrchných alebo spodných okrajoch obrázku. Navyše, znaky sú postavené vedľa seba horizontálne, nikdy nie vertikálne. Na základe týchto pozorovaní dokážeme určiť relatívne umiestnenie znakov v obrázku a určiť a odstrániť väčšinu kriviek a čiar.



**Obr. 4.4: Postupná segmentácia podľa farebnej výplne na kusy. Prevzaté z [28].**

Po rozdelení do kusov sa jednotlivo na každý kus uplatňuje odstraňovanie kriviek a čiar. Príklad vidíme na obrázku 4.5, na ktorom sa nachádzajú tri objekty, pričom dva z nich (písmená U a A) sú viac-menej zoradené podľa určitej bázovej línie a tretí objekt (čiara) sa nachádza nad oboma týmito objektmi, preto je odstránený.

**Obr. 4.5: Odstraňovanie kriviek. Prevzaté z [28].**

## 4.3 Útok presmerovaním

V kontexte Captcha známy aj ako „*pornografický útok*“. Myšlienka útoku je v zautomatizovaní všetkého, čo sa dá, hoci samotná Captcha je riešená človekom. Demonštrujme tento útok pri registrácii účtu v službe *Gmail*, ktorú označíme ako *G*. Registrácia obsahuje Captcha založenú na rozpoznávaní textu. *Server*, ktorý útok vykoná, označíme ako *E*. Predpokladom je, že *užívateľ A* ma záujem o zobrazenie stránky od *E*:

1. *A* pošle cez HTTP požiadavku o načítanie web stránky od *E*,
2. *E* načíta web stránku *G* a dostane HTML kód danej stránky. Keďže jeho štruktúru vopred pozná, vie ho sparsovať[11] tak, aby dostal URL adresu, na ktorej je vygenerovaný obrázok konkrétnej inštancie Captcha pre danú reláciu (ktorú začal *E*, keď požiadal o načítanie stránky *G*),
3. *E* posiela *A* späť HTML kód s formulárom, ktorý obsahuje <*img*> element ukazujúci na danú vygenerovanú Captcha a textové políčko, kde očakáva odpoveď s odôvodnením, že ak chce *A* vidieť skutočný obsah stránky od *E*, musí najskôr prepísať text, ktorý vidí na obrázku,
4. *A* pošle odpoveď *E*,

[11] **parsovanie** alebo **parsing** je spôsob, ako zo vstupného reťazca dostať do patričných premenných informácie zakódované v tomto reťazci. Zdroj: http://kam.mff.cuni.cz/~kuba/vyuka/programovani

5. *E* prepošle odpoveď od *A* spolu s ďalšími údajmi potrebnými na registráciu (meno, heslo, ...), ktoré zvolil sám *E*, serveru *G*,
6. *G* pošle odpoveď *E*,
7. *E* vie, že môže dostať 2 typy odpovede – *A* vyriešil Captcha správne a registrácia bola úspešná, alebo bola registrácia zamietnutá. V prvom prípade pošle *E* stránku, o ktorú *A* v prvom kroku požiadal, v druhom prípade pošle chybovú hlášku alebo sa pokúsi zopakovať postup od druhého kroku.

Variáciou na tento systém je, že motivácia užívateľa *A* nespočíva v záujme obsah stránky od *E*, ale sú ňou peniaze. Je mu zobrazená jedna Captcha za druhou a po správnom riešení sa mu na účet pripíše určitá suma. Takýto systém nie je prelomením Captcha a jeho jediné využitie je biznis. To je súčasne aj jeho slabinou, pretože útočník musí byť schopný vyťažiť zo získanej vyriešenej Captcha viac, ako sú jeho náklady na motivovanie človeka, ktorý ju má vyriešiť. [25]

# Kapitola 5

## Vlastnosti ideálnej Captcha

Napriek mnohým rokom vývoja a používania, sa Captcha ešte stále javí byť ďaleko od dokonalého riešenia. Ideálna Captcha je žiadna Captcha – teda najlepším riešením by bolo odstrániť motiváciu k spamu, aby spam prestal byť lukratívnym prostriedkom k jednoduchému obohacovaniu, a Captcha by viac nebola potrebná. Kdežto kedysi bola Captcha jednoduhý text na bielom podklade, ktorý stačilo prepísať, v súčasnosti je zameraná viac na elimináciu spamu, ako na potvrdenie, že test rieši ľudský užívateľ. A pokiaľ spamer nie je počítač, je Captcha neúčinná. Spameri totiž často využívajú ľudskú silu, majú doslova plné miestnosti nízko nákladových zamestnancov, ktorí jednoducho ťukajú a skúšajú riešiť Captcha.[15] Na takom princípe fungujú napríklad weby BeatCaptchas.com alebo CaptchaBuster.com. V súčasnej dobe je ale spam, rovnako ako napríklad vírus chrípky, prirodzenou súčasťou internetu a jeho prítomnosť jednoducho súvisí so slobodou a neurčitosťou celého internetu. Zjednodušene povedané ale platí, že úsilie vynaložené na vytvorenie Captcha nesmie byť väčšie, ako úsilie vynaložené na jej prelomenie.

## 5.1 Kritériá použiteľnosti

Capcha sa v priebehu rokov menila a z relatívne jednoduchého a triviálneho testu sme sa dostali do fázy, kedy v extrémnom prípade užívateľ nie je schopný Captcha vyriešiť a teda nedokáže naplniť cieľ interakcie. To je fatálna chyba v použiteľnosti, ku akým by nemalo dochádzať. Nasledovné kritériá sú interpretované v rovine použiteľnosti Captcha bez ohľadu na rôzne problémy, ktoré môžu vzniknúť pri implementáciách v niektorých programoch alebo webových stránkach. Požiadavky na schopnosť používania podľa normy ISO 9241-11 [9] sú: *efektívnosť*, *časová hospodárnosť* a *spokojnosť*. Pre potreby Captcha boli rozšírené o kvalitatívne prvky: *naučiteľnosť*, *zapamätateľnosť* a *zabránenie chybám*. Chyby pri riešení Captcha sa sa vzťahujú na náročnosť riešenej Captcha a zjednodušenie Captcha-problému kvôli vylepšeniu použiteľnosti sa prejaví negatívne na ochrane pred automatizovanými útokmi, pred ktorými nás ma chrániť.

Preto posledné menované kritérium v tejto súvislosti nie je interpretované ako aspekt použiteľnosti ale ako vnútorný aspekt problému riešenia, a v tomto kontexte kvantitatívne vyjadrenie zabránenia chybám chápeme ako čiastkový aspekt kritéria efektívnosť.

Užívateľský test, uskutočnený v roku 2012 v Nemecku [8], mal za cieľ vyhodnotiť niektoré Captcha systémy podľa kritérií použiteľnosti a pozostával z 50 testovaných osôb, ktoré boli rozdelené do dvoch skupín: „študenti a „ostatní“, teda neštudujúci v zmiešanej vekovej kategórii.

| Všetci účastníci | |
|---|---|
| Skupina | Počet |
| Študenti | 25 |
| Ostatní | 25 |
| Vek | Počet |
| 14-19 | 6 |
| 20-29 | 30 |
| 30-39 | 2 |
| 40-49 | 10 |
| 50-59 | 2 |
| nad 60 | 0 |
| Využívanie internetu | Počet |
| málo | 12 |
| normálne | 26 |
| často | 12 |

| Skupina „Študenti“ | |
|---|---|
| Vek | Počet |
| 14-19 | 1 |
| 20-29 | 24 |
| 30-39 | 0 |
| 40-49 | 0 |
| 50-59 | 0 |
| nad 60 | 0 |
| Využívanie internetu | Počet |
| málo | 0 |
| normálne | 15 |
| často | 10 |

| Skupina „Ostatní“ | |
|---|---|
| Vek | Počet |
| 14-19 | 5 |
| 20-29 | 6 |
| 30-39 | 2 |
| 40-49 | 10 |
| 50-59 | 2 |
| nad 60 | 0 |
| Využívanie internetu | Počet |
| málo | 12 |
| normálne | 11 |
| často | 2 |

**Tabuľka 2 – Demografický prehľad účastníkov testu. Prebraté z: [8].**

Všetci zúčastnení boli oboznámení s obsluhou počítača a periférií. V rámci možností boli testovaní vyberaní náhodne, všetci sa zúčastnili dobrovoľne. Test bol prevedený

v klasických laboratórnych podmienkach, čo znamená napríklad opticky pokojné zóny, v ktorých sa testovaní mohli plne sústrediť na riešenie zadaných úloh. Každý typ Captcha bol následne riešený v troch kolách. Medzi testovanými Captcha systémami musel byť vykonaný výber, pretože nie všetky spĺňali požiadavky na tento test – z praktických dôvodov neboli zohľadnené Captcha systémy čisto v anglickom jazyku, alebo také, ktoré nie sú voľne dostupné. Test teda obsahoval nasledovné Captcha systémy: Google reCaptcha (v teste rozdelená do 2 častí – obrazová časť ako *textová Captcha* a zvuková časť ako *zvuková Captcha*), *obrázková* Microsoft Asirra, *reklamná* CaptchaAd a jednoduchá *matematická* Captcha [8].

| | |
|---|---|
| **Efektívnosť** | Aká vysoká je miera rozpoznateľnosti? Koľko pokusov užívateľ potrebuje, aby Captchu úspešne vyriešil? |
| **Časová hospodárnosť** | Akú priemernú dobu trvá správne vyriešenie Captche? Dokáže byť úspešne vyriešená do 30 sekúnd? |
| **Naučiteľnosť** | Dokáže užívateľ na prvý pohľad rozoznať, akým spôsobom má byť Captcha korektne použitá a riešená? |
| **Zapamätateľnosť** | Ako dobre si dokáže užívateľ spomenúť na koncept Captche? |
| **Spokojnosť** | Ako ľahko/ťažko užívateľ nájde Captchu? Cítia sa užívatelia pri jej používaní dobre? Aký poskytujú feedback? |

**Tabuľka 3: Formalizované kritériá použiteľnosti. Prevzaté z [8].**

### 5.1.1 Efektívnosť

Kvantifikovateľná merná veličina pre dáta k efektívnosti je *miera rozpoznania*. Tá je definovaná ako podiel úspešných riešení a všetkých pokusov. V tomto aspekte zvíťazila matematická Captcha s mierou rozpoznania na úrovni 98,67% a za ňou nasledovali textová Captcha s hodnotou miery rozpoznania 92%, Microsoft Asirra s výsledkom 84%, CaptchaAd s hodnotou 74% a zvuková Captcha 68,87%. Efektívnosť bola testovaná v spoločnej testovacej skupine, každý Captcha variant bol pozorovaný 150krát. Zaujímavosťou je, že matematická Captcha dosiahla v skupine študentov mieru rozpoznania 100%. Pri účastníkoch vo vekovej kategórii 50-59 rokov bolo korektne vyriešená iba tretina testov Microsoft Asirra.

| Typ Captcha | Miera rozpoznania (%) |
|---|---|
| **matematická** | 98,67 |
| **textová** | 92,00 |
| **Asirra** | 84,00 |
| **CaptchaAd** | 74,00 |
| **zvuková** | 68,87 |

**Tabuľka 4: Výsledky podľa miery rozpoznania**

### 5.1.2 Časová hospodárnosť

Aj pri pozorovaní časovej hospodárnosti sa pomyselným víťazom stala matematická Captcha ako najpriaznivejšia zo skúmaných alternatív. Správne bola totiž vyriešená v priemere len za 7,27 sekúnd. Na vyriešenie textovej Captcha potreboval užívateľ priemerne čas 17,63 sekúnd, teda o viac než 10 sekúnd viac. S 25,9 sekundami nasleduje Microsoft Asirra, reklamná CaptchaAd s 29,48 sekundami a nakoniec zvuková Captcha s 36,18 sekundami. Zaujímavé je, že v prípade matematickej aj CaptchaAd užívatelia potrebovali viac času na nesprávne riešenie, naopak správne riešenie vyplnili rýchlejšie.

| Typ Captcha | Čas na vyriešenie (s) |
|---|---|
| **matematická** | 7,27 |
| **textová** | 17,63 |
| **Asirra** | 25,90 |
| **CaptchaAd** | 29,48 |
| **zvuková** | 36,18 |

**Tabuľka 5: Výsledky podľa času potrebného na vyriešenie**

### 5.1.3 Naučiteľnosť

Ako rozmer pre naučiteľnosť je pri Captcha *miera využívania nápovedy* v daných systémoch. Pri usporiadaní podľa frekvencie vyvolávania nápovedy sa nám ukazuje iný obraz, ako pri *miere rozpoznania*. Kým matematická Captcha vykazovala najvyššiu mieru rozpoznania, nápoveda bola využitá v 6% prípadov. Vyššiu hodnotu dosiahli CaptchaAd s 11,33% a Microsoft Asirra s 6,67%. Pri zvukovej Captcha dosiahla miera využívania nápovedy 4,67% a pri textovej Captcha len 2,67%. Pri tomto kritériu boli zaznamenané pomerne značné rozdiely v testovaných skupinách – kým v skupine „študenti“ bola funkcia pomoci použitá len jediný raz, a to v prípade zvukovej

Captcha, v skupine „ostatní“ sa využívala hojnejšie. Domnienka je, že s narastajúcim vekom sa zvyšuje aj využívanie nápovedy.

| Typ Captcha | Miera využívania nápovedy (%) |
|---|---|
| **textová** | 2,67 |
| **zvuková** | 4,67 |
| **matematická** | 6,00 |
| **Asirra** | 6,67 |
| **CaptchaAd** | 11,33 |

**Tabuľka 6: Výsledky podľa miery využívania nápovedy**

### 5.1.4 Zapamätateľnosť

Zapamätateľnosť nejakého Captcha systému sa ukazuje ako doba potrebná na vyriešenie Captcha testu v priebehu času (resp. po opakovaní kôl v priebehu testu). Všetky testované metódy vykázali v priebehu času pokles doby potrebnej na vyriešenie testu. Najväčšie rozdiely, teda závislosť medzi poradím kola a dobou potrebnou na vyriešenie, sa ukázali pri Microsoft Asirre, matematickej a zvukovej Captcha, naopak najmenší efekt opakovania testu ukázala textová Captcha. Pravdepodobne užívatelia tejto metóde natoľko dôverujú a poznajú ju, že ďalšie skúsenosti pri opakovaní testu už nemajú vplyv na dobu potrebnú na vyriešenie Captcha.

### 5.1.5 Spokojnosť

Na konci celého testu bola skúmaná spokojnosť pokusných osôb, ktoré hodnotili jednotlivé Captcha systémy známkami ako v škole, teda na škále 1 až 5, pričom hodnota 1 vyjadruje najväčšiu spokojnosť. Ako najhoršia sa ukázala zvuková Captcha s hodnotou 2,85, ktorú nasleduje CaptchaAd s výsledkom 1,85. Textová Captcha bola ohodnotená priemernou známkou 1,72. Nasleduje Asirra s výsledkom 1,44 a matematická Captcha, ktorá získala priemernú známku 1,11. Matematická Captcha nezískala ani v žiadnom jednotlivom hodnotení spokojnosti horšiu známku ako 3, Microsoft Asirra zase nikdy nezískala žiadnu 5. Naopak zvuková Captcha bola len málo testovanými osobami hodnotené ako „ľahko riešiteľná“, čomu zodpovedá aj najvyšší počet zlých známok.

Testovaní mali na konci testu takisto možnosť otvorenej odpovede, v ktorej mohli vyjadriť postrehy, ktoré sa nedajú zhrnúť do štruktúrovaných otázok. Štyria účastníci považovali zvukovú Captcha za príliš ťažkú alebo nezrozumiteľnú. Ďalší účastník ju označil za obtiažnu a zdĺhavú a náchylnú na omyl a z týchto dôvodov nie príliš praktickú. Dvaja účastníci zhodnotili zvolené otázku v CapchaAd ako nie dostatočne precízne vybranú, teda nevedeli, ktorá z informácií je správnou odpoveďou. Iní traja zúčastnení označili Microsoft Asirra ako príjemnú a ľahko zvládnutú, jeden sa naproti tomu z nej cítil vynervovaný. Jeden účastník označil textovú Captcha ako ťažko čitateľnú, iný zúčastnený považuje matematickú Captcha za nie bezpečnú. [8]

| Typ Captcha | Spokojnosť (známka) |
|---|---|
| **matematická** | 1,11 |
| **Asirra** | 1,44 |
| **textová** | 1,72 |
| **CaptchaAd** | 1,85 |
| **zvuková** | 2,85 |

**Tabuľka 7: Výsledky podľa spokojnosti užívateľov**

## 5.2 Kvalitatívne kritériá

Malé stránky sa dokážu efektívne chrániť aj použitím niekoľkých otázok typu „Akej farby je nebo?“. Kým útočník nemá dôvod „otestovať“ daný web, stačí to na zastavenie skriptov, ktoré do rôznych komentárov posielajú spam. Ak sa ale bavíme o kvalitnej Captcha, musí mať určité kvalitatívne vlastnosti, ktoré sa pokúsim zhrnúť. Je ale dôležité povedať, že tieto kritériá určite nie sú jediné a rôzne zdroje sa v taxonómii mierne líšia.

### 5.2.1 Prostredie

Vhodným prostredím rozumieme také prostredie, ktoré spĺňa všetky podmienky, aby v ňom daná Captcha bezproblémovo fungovala. Hoci väčšina Captcha implementácii funguje na bázi štandardov HTML, problémy môže spôsobiť napríklad použitie CSS alebo Adobe Flash. Aj napriek tomu, že dnes sú už štandardným vybavením prehliadačov, ideálna Captcha by mala byť vytvorené spôsobom *postupného*

*vylepšovania* (*progressive enhancement*[12]), to znamená, že bude fungovať aj na tom najslabšie vybavenom prehliadači, hoci v jednoduchšej verzii.

Je nutné doplniť, že niektoré Captcha testy si v snahe príliš neobťažovať užívateľa ukladajú úspešne vyriešený test do *cookie*[13] a daného užívateľa viacej nekontroluje. Po jednoduchom (reverzibilnom) kódovaní sa však dá k údajom dostať. Pri odoslaní užívateľovi môže byť toto riešenie dekódované jednoduchšie, ako pokus s OCR. [16] Tiež musí platiť, že po každom neúspešnom pokuse o vyriešenie Captcha sa musí vygenerovať nová inštancia.

### 5.2.2 Bezchybnosť

*Chyba typu I* a *Chyba typu II* sú presné technické pojmy používanej štatistiky na popísanie konkrétnych chýb v testovacom procese, kde niečo, čo malo byť prijaté, bolo odmietnuté, a kde niečo, čo malo byť odmietnuté, bolo prijaté. V teórii štatistických testov je pojem štatistická chyba neoddeliteľnou súčasťou testovania štatistických hypotéz. Pokiaľ výsledok testu korešponduje so skutočnosťou, tak bolo učinené správne rozhodnutie. Ale v prípade, ak výsledok testu nekorešponduje so skutočnosťou, vtedy nastala chyba. Kvôli štatistickej povahe testu sa chyba vo výsledku, až na vzácne prípady, nedá úplne vylúčiť. Rozlišujeme dva typy chýb: *chyba typu I* a *chyba typu II*.

#### 5.2.2.1 Chyba typu I

*Chyba typu I*, inak známa ako chyba prvého druhu, je chybné rozhodnutie učinené po tom, čo test odmietne pravdivú hypotézu H. Chyba typu I sa taktiež označuje ako *false positive*. Chyba typu I môže byť vyjadrená ako chyba nadmernej dôveryhodnosti. [18] Pri hypotéze H: *„Človek rieši Captcha“* nastáva chyba typu I vtedy, ak človek Captcha nevyriešil, alebo ju vyriešil nesprávne, ale napriek tomu testom prejde.

[12] **Progressive Enhancement -** na samotnom začiatku designujeme aplikáciu tak, aby bola použiteľná vo všetkých prehliadačoch aj bez javascriptu. A pomaly pridávame, najčastejšie práve pomocou podmienenej server verzie kódu, javascriptu a css. Dôležité je, že nech sa deje čo sa deje, vždy máme niečo, čo je použiteľné všade. Zdroj: http://www.vyvojari.sk/news-tvorba-rozhrania-webu-pomocou-techniky-progressive-enhancement-101381.aspx

[13] **cookie** - v protokole HTTP malé množstvo dát, ktoré WWW server pošle prehliadaču, ktorý ich uloží v počítači užívateľa. Pri každej ďalšej návšteve rovnakého serveru potom prehliadač tieto dáta posiela späť serveru. Zdroj: Wikipedia

Príkladom Captcha náchylnej k vysokej miere chyby typu I je taká Captcha, ktorá pre užívateľa úplne nečitateľná a teda nevyriešiteľná.

#### 5.2.2.2 Chyba typu II

*Chyba typu II*, tiež známa ako chyba druhého druhu, je chybné rozhodnutie učinené, keď test zlyhá v odmietnutí falošnej nulovej hypotézy H. Chyba typu II býva označovaná aj ako *false negative*. Chyba typu II môže byť vyjadrená ako chyba nadmerného skepticismu. [18] Pri hypotéze H: *„Človek rieši Captcha"* nastáva chyba typu II vtedy, ak Captcha nerieši človek, ale počítač a ten prejde testom. Príkladom Captcha náchylnej k vysokej miere chyby typu II je taká Captcha, ktorá je triválne prelomiteľná pomocou technológie OCR.

### 5.2.3 Náročnosť

Je veľmi dôležité, aby Captcha nebola prehnane zložitá. Už z definície sa jedná o test, ktorý má byť *„ľahký pre človeka, ale zložitý pre počítač"*. Musí sa preto dbať na to, aby bola Captcha pre ľudského užívateľa bez vážnejších problémov riešiteľná, v opačnom prípade spôsobuje frustráciu užívateľa, v najhoršom prípade jeho odchod z danej stránky. Užívatelia tiež nie sú ochotní stráviť nad riešením (z ich laického pohľadu zbytočného) Captcha testu viac času, ako je nevyhnutné. Hoci krátka alebo dlhá doba na vyriešenie Captcha sú relatívne pojmy, je potrebné, aby bolo pre užívateľa jasné zadanie úlohy (napr. „Prepíš text z obrázku", „Označ mačku na fotografii" atď.) a aby samotná úloha nebola priveľmi zložitá, príliš náročná na čas alebo dokonca neriešiteľná. Vhodným doplnkom je možnosť obnovenia (*refresh*) Captcha, teda vygenerovanie nového testu, pokiaľ sa užívateľovi zobrazila (subjektívne alebo objektívne) ťažko riešiteľná Captcha.


**Obr. 5.1: Príklad príliš náročnej Captcha.**

**Prevzaté z http://markhaase.com/2012/08/30/recaptcha-is-a-blight/**

### 5.2.4 Prístupnosť

Pravidlá prístupnosti sú v Českej republike zakotvené aj v novele *Zákona č. 365/2000 Sb. o informačních systémech veřejné správy*, vykonanou zákonom č. 81/2006 Sb. Podľa nej: *„Ak je obrázok použitý kvôli odlíšeniu, či so stránkou pracuje skutočný človek alebo počítač (tzv. Captcha), sú užívateľovi k dispozícii i doplnkové metódy, ktoré umožňujú toto odlíšenie vykonať (napr. zvukový výstup atp.)“* [17]. Preto, aby bol zachovaný čo možno najviac rovnocenný prístup aj pre ľudí s nejakým handicapom, väčšinou sa stretávame so zvukovou alternatívou, kde však narážame na problém, že rozpoznávanie hlasu môže byť často jednoduchšie, ako rozpoznávanie textu. Za zváženie stojí napríklad automatické telefonovanie, ako iná alternatíve ku zvukovej Captcha, alebo autorizácia pomocou SMS v prípade, ak užívateľ nie je schopný dokončiť vizuálnu Captcha. Hoci ani to nezaručuje patričnú prístupnosť, keďže užívateľ môže mať potenciálne viacero handicapov. Samozrejme je rovnako dôležité, aby bol pre handicapovaného človeka rovnako prístupný celý web, nielen samotná Captcha.

## 5.3 Ďalšie kritériá pre Captcha založenú na rozpoznávaní textu

Tento typ tvorí drvivú väčšinu v súčasnosti používaných Captcha systémov a s jeho popularitou priamo úmerne narastá aj záujem útočníkov, čo dokazujú aj mnohé pokusy o jej prelomenie.[19][20] Aj to vedie k tomu, že sa používajú čoraz väčšie deformácie, čo spôsobuje nárast chýb prvého druhu. Práve pre najväčšie zastúpenie tohto typu Captcha, zhrniem ďalšie vlastnosti, ktoré by mala mať silná a ideálna Captcha založená na rozpoznávaní textu.

### 5.3.1 Výber písma, sady znakov a slov

Aby sme útočníkovi neuľahčili prácu, treba dbať aj na výber vhodného písma. Nevhodnými písmami sú *pätkové písma* (*serif*), pretože pätky[14] často obsahujú jedinečné

[14] **Pätky písma** (angl. serif) - sú kolmé zakončenia ťahov písmen, ktoré vizuálne pomáhajú držať rovinu riadka. Zdroj: http://tvorim.net/typografia/70-pisma-delenie-fontov-a-ich-primerane-pouzitie

ťahy typické práve pre konkrétny znak abecedy. Preto sú odporúčané graficky jednoduchšie *bezpätkové písma* (*sans-serif fonts*).


**Obr. 4.2: Príklad pätkového písma a jedinečných zakončení niektorých znakov.**
**Prebraté z: [16].**

Čo sa týka použitej sady znakov, typicky sa odporúča použiť celú alfanumerickú škálu, s prípadnou výnimkou znakov 0 (nula) a O (veľké tlačené písmeno o). Typicky, čím je použitá sada znakov širšia, tým je odolnosť voči útoku uhádnutím nižšia. Je vhodné použiť také písmo, aby pre čo najviac znakov existovala viac ako jedna možnosť rozoznania, čo výrazne zvýši odolnosť voči OCR.

Naopak odolnosť voči OCR znižuje používanie tzv. slovníkových slov, teda plnovýznamových slov, ktorých zoznam sa dá nájsť v slovníkoch. Pi používaní týchto slov, predovšetkým pri dlhších slovách, existuje riziko, že pri rozoznaní väčšiny znakov pomocou OCR sa spustí knižnica kontroly pravopisu a vyberie najpravdepodobnejší návrh slova. Používanie slovníkových slov sa teda neodporúča, rovnako ako sa neodporúča používať príliš krátke reťazce slov.

### 5.3.2 Nadbytočné medzery

Možno triviálna vec, ktorá ale dokáže útočníkovi mnohonásobne uľahčiť prácu, sú medzery medzi jednotlivými znakmi v textovej Captcha. Dovoľuje mu to použiť tzv. *útok hrubou segmentáciou* (*rough slicing attack*), kedy sa hľadajú ohraničujúce rámce jednotlivých znakov približnej veľkosti a potom sa redukujú, kde je to možné. Preto je veľmi dôležité zamedziť väčším medzerám medzi znakmi, ktoré by sa mali prekrývať, pretože po aplikovaní segmentácie je rozoznanie jednotlivých znakov pre počítač oveľa jednoduchšou úlohou, ako pre človeka.

**Obr. 5.3: Príklad Captcha s nadbytočnými medzerami a segmentácia pomocou ohraničujúcich rámcov.**

**Prebraté z: [16].**

### 5.3.3 Rušivý šum a doplňujúce línie

V pozadí by mal byť použitý *rušivý šum* (*noise*), ktorý však nesmie byť taký, aby príliš znížil čitateľnosť pre človeka. Je vhodné, aby pri generovaní jednotlivých inštancií nebolo vždy používané rovnaké pozadie, pričom pozadie by malo rozbíjať kontúry znakov.


**Obr. 5.4: Príklad nesprávne zvoleného pozadia.**

**Prebraté z: [16].**

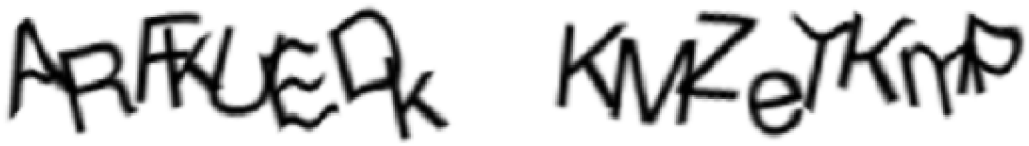
Ďalším dôležitým prvkom je používanie takzvaných *rušivých línií* (*noise lines*). Môžeme si pod nimi predstaviť rôzne čiary alebo krivky. Tieto by mali mať rovnakú hrúbku a štruktúru ako slovo, alebo ak je slovo deformované a má rôznu hrúbku čiar, mala by sa meniť aj hrúbka použitých rušivých línií. Línie by mali viesť rovnakým smerom ako ťahy, ktoré tvoria písmená. Často sa stáva, že sú tieto línie pritenké a pomocou techník *stenčovania* (*erode*) a *zhusťovania* (*dilate*) je možné jednoducho sa ich zbaviť.


**Obr. 5.5: Príklad nesprávne zvolených rušivých línií a ich odstránenie.**

**Prebraté z: [16].**

### 5.3.4 Otočenie a skrivenie jednotlivých znakov

Zdá sa, že pri väčšine implementácií sa univerzálnym prístupom stalo generovanie náhodného textu a aplikovanie jednoduchých filtrov, ktoré tento text deformujú, napríklad skrútenie (*warp*). Zabúda sa na to, že všetky takéto operácie sú reverzibilné. Ak chceme urobiť Captcha odolnejšou voči OCR, zdá sa byť otočenie a skrivenie jednotlivých znakov v kombinácii s prekrývaním (*overlap*) ako najlepšie riešenie. V tomto prípade teda útočník musí prejsť ku segmentácii bez pokusu o reverznú funkciu, resp. ku segmentácii prejde po neúspešnom pokuse o odstránenie deformácie. Najlepší výsledok vzniká pri vytvorení jednotlivých znakov a línií na priehľadnom (transparentnom) pozadí a následné aplikovanie deformácie skrútením (*warp*).



**Obr. 5.6: Príklad Captcha pri otočení a skrútení jednotlivých znakov.**

**Prebraté z: [16].**

## 5.4 Vyhodnotenie

V tejto kapitole sme doteraz popísali kritériá, ktoré by v ideálnom prípade Captcha mala spĺňať. V druhej kapitole sme popísali 7 typov Captcha (za ôsmy budeme vo vyhodnotení považovať zvukovú Captcha, hoci sa zvyčajne používa iba ako doplnková) a tie teraz podľa vyššie určených kritérií zhodnotíme.

Začneme hodnotením kritérií použiteľnosti. Keďže však nie sme schopní nasimulovať podmienky, ktoré by boli ekvivalentné s tými nemeckými, v ktorých sa test na tieto kritériá uskutočnil, niektoré nami predstavené typy Captcha do tohto testu nie sú zahrnuté a príslušné bunky tabuľky sú z tohto dôvodu prázdne.

| | Efektívnosť | Časová hospodárnosť | Naučiteľnosť | Zapamätateľnosť | Spokojnosť |
|---|---|---|---|---|---|
| textová | ✓ | ✓ | ✓ | ✓ | ✓ |
| obrázková | O | ✓ | ✓ | - | ✓ |
| matematická | ✓ | ✓ | ✓ | - | ✓ |

| | | | | | |
|---|---|---|---|---|---|
| **animovaná** | | | | | |
| **puzzle** | | | | | |
| **rozpoznávanie priateľov** | | | | | |
| **reklamná** | O | O | O | - | ✓ |
| **zvuková** | O | x | x | - | x |

**Tabuľka 8: Vyhodnotenie kritérií použiteľnosti**

Legenda: ✓ spĺňa danú požiadavku
O čiastočne spĺňa danú požiadavku
x nespĺňa danú požiadavku
- nie je možná žiadna odpoveď

Z vyššie uvedenej tabuľky nám jednoznačne vychádza, že užívatelia najlepšie hodnotia práve Captcha založenú na rozpoznávaní textu. Dá sa predpokladať, že veľmi dobré výsledky by v tomto smere dosiahla aj Captcha s rozpoznávaním priateľov, avšak táto je žiaľ zatiaľ použiteľná iba pre užívateľov sociálnej siete Facebook a teda nie je univerzálnym riešením, na základe čoho sa domnievam, že niektorí účastníci nemeckého testovania, ktorí sú neznalí tejto sociálnej siete, by mohli byť neúspešní. Vychádzam i z výsledkov dosiahnutých v tomto teste Asirrou.

Ďalej sa zameriame na hodnotenie kvalitatívnych kritérií. Tieto sú rovnako ako kritériá použiteľnosti, ak nie ešte viac, závislé od konkrétnej implementácie a preto nie je jednoduché hodnotiť každý typ rámcovo ako celok. Ešte si pripomenieme tieto kritériá, sú to: prostredie, chyba typu I, chyba typu II, náročnosť a prístupnosť.

Textová Captcha je asi najviac rozdielna v závislosti od implementácie. Preto nie je možné zhodnotiť kritérium prostredie – ideálne by malo byť nenáročné. Dobré prevedenie textovej Captcha je nenáchylné k chybám typu II, čo ale zvyšuje pravdepodobnosť chyby typu I. Náročnosť je variabilná, v súvislosti s týmto typom Captcha sme sa jej už viackrát venovali. Prístupnosť je zväčša vyhovujúca, keďže v praxi je súčasťou väčšiny týchto testov aj zvuková varianta.

Obrázková Captcha, reprezentovaná Asirrou a KittenAuth je nenáročná na prostredie, realizované sú cez HTML. Sú náchylnejšie na chyby typu II a to z dôvodu malej množiny odpovedí na konkrétnu inštanciu. Náročnosť hodnotím subjektívne ako pomerne nízku, hoci test použiteľnosti pri Asirre prekvapil trochu inými výsledkami. Nespĺňa kritérium použiteľnosti, keďže neobsahuje inú variantu testu.

Matematická Captcha je nenáročná na prostredie a nenáchylná k chybám typu I (pri jednoduchých matematických úlohách), avšak náchylnejšia k chybám typu II. Tým sa dá zabrániť napríklad lepšími deformáciami, podobne ako pri Captcha založenej na rozpoznávaní textu. Náročnosť je závislá od konkrétnej implementácie, od elementárnych počtov („2+2“) až po príliš náročný test, zobrazený v kapitole 2. Väčšina týchto Captcha, s ktorými som sa stretol, nespĺňali kritérium prístupnosti.

Reklamná, puzzle a animovaná Captcha sú typy, ktoré sú zaujímavejšie skôr vizuálne, čo ale zvyšuje ich náročnosť na prostredie. Samotná náročnosť testu sa mení od prípadu k prípadu, osobne si však myslím, že pre bežného internetového užívateľa by náročnosť mohla byť vyššia (i keď to už zachádzame viac do kritérií použiteľnosti). Všetky tieto typy nespĺňajú ani kritérium prístupnosti. Celkovo sú tieto typy využívané v menšej miere.

Typ rozpoznávanie priateľov nebudeme bližšie hodnotiť. Ako už bolo spomenuté, jedná sa zatiaľ o internú záležitosť sociálnej siete, ktorá ešte dozaista podľahne mnohým zmenám a úpravám. Pravdepodobne je ale nenáchylná k chybám typu I a II.

Zvuková Captcha, ak je použitá samostatne, nespĺňa kritérium prístupnosti, keďže nie je riešiteľná pre ľudí s problémami sluchu. Pri použití primeraných transformácií je náročnosť primeraná, situácia je veľmi podobná ako pri Captcha založených na rozpoznávaní textu. Rovnako sú, pri kvalitnej implementácii, náchylnejšie na chybu typu I ako II.

Pomyselným víťazom teda označujem Captchu založenú na rozpoznávaní textu. Hoci sa nejedná o užívateľsky najzaujímavejšiu a vizuálne najatraktívnejší typ (čo ani nie je primárnym cieľom Captcha ako takej, avšak z užívateľského hľadiska by to samozrejme bolo príjemné), ukazuje sa tento najstarší typ ako najvhodnejší podľa nami zvolených kritérií. Textovú Captcha preto za predpokladu, že spĺňa kritériá určené v tejto kapitole, môžeme označiť za ideálnu Captcha.

# Kapitola 6

## Vylepšená Captcha

V súčasnosti neexistujú štatistiky, ktoré by hovorili niečo o tom, v akej miere je celkovo na weboch využívaná technológia Captcha. Pre bežného autora webových stránok je všeobecne lepšie použiť už existujúcu implementáciu Captcha, ako vyvíjať novú. Už prvá Captcha, vytvorená v roku 1997 pre vyhľadávanie AltaVista, bola založená na rozpoznávaní textu. Hoci dnes máme na výber z rôznych druhov tohto obráteného Turingovho testu, podľa môjho názoru je kvalitne vytvorená textová Captcha stále tou najlepšou variantou, ako sme k tomu dospeli aj po vyhodnotení požiadaviek a kritérií ideálnej Captcha.

Vytvoriť kvalitnú Captcha založenú na OCR nie je ľahké. V 5.3 sa venujeme najdôležitejším bodom, ktoré je nutné dodržať. Neprípustné sú veľké medzery medzi jednotlivými znakmi, takisto neprípustné sú deformácie aplikované na celý reťazec znakov naraz – je nutné deformovať každý znak osobitne. Captcha je vytvorená v jazyku PHP[15], ktorý je nezávislý na platforme, je najrozšírenejším skriptovacím jazykom s jednoduchou syntaxou. Cieľom bolo, aby bola nenáročná na prostredie a pretože HTML nepodporuje natívnu podporu prehrávania zvukov, z tohto dôvodu táto Captcha neobsahuje zvukovú alternatívu a teda nespĺňa pravidlo prístupnosti. Zámer bol vyhnúť sa technológiám ako Flash, QuickTime alebo Silverlight. Captcha je vo forme jednoduchého formuláru, kde je užívateľovi ukázaný obrázok a on má prepísať text z neho. Captcha obsahuje odkaz „Refresh image“ slúžiaci na obnovu obrázku v prípade, že daná inštancia je pre užívateľa z akéhokoľvek dôvodu nečitateľná. Dôležitým prvkom sú rušivé línie – krivky a čiary, ktoré sa snažia dopĺňať znaky tak, aby boli ešte stále čitateľné pre človeka, ale mätúce pre OCR. Rôzne inštancie Captcha sú vytvorené za použitia niekoľkých písiem, spravidla bezpätkových. Znaky O a 0 sú vynechané. Z hľadiska kritérií použiteľnosti vyšla textová Captcha najlepšie aj spomedzi užívateľského testu, spomínaného v kapitole 5.

[15] **PHP** (PHP: Hypertext Preprocessor) je open source skriptovací programovací jazyk, ktorý sa používa najmä na programovanie klient-server aplikácií a pre vývoj dynamických webových stránok. Zdroj: Wikipedia

Za najväčší nedostatok považujem, že obrázky nie sú generované, ale sú vybraté z dopredu vytvorenej databázy. Keďže sa však jedná o pokus o vylepšenie, ktorý má ukázať, akým smerom je možné sa vyberať a ako by mala vyzerať Captcha pri snahe o dodržanie väčšiny kritérií formalizovaných v kapitole 5, a Captcha je funkčná, nepovažujem to za nenaplnenie zadania. Na prvý pohľad sa môže zdať, že niektoré inštancie sú náchylné na chybu typu I, avšak po zadaní tohto testu mojím (informatikou sa nezaoberajúcim) známym, ktorí všetci úspešne vyriešili aj inštancie, ktoré som osobne považoval za náchylné na chybe typu I. Pravdepodobnosť chyby typu II je veľmi nízka.

**Obr. 6.1: „DSURA“**

**Obr. 6.2: „tyf8r“**

**Obr. 6.3: „8ZKE6“**

# Záver

Táto práca bola venovaná technológii Captcha. Výsledkom práce je teoretický prehľad vybraných typov Captcha so zameraním na vlastnosti ideálnej Captcha. Najmä z hľadiska prístupnosti, ale aj z iných, sa ako najlepší javí typ založený na rozpoznávaní textu, hoci sa dá namietať jeho nezaujímavosťou. Druhým výsledkom práce je praktická časť – pokus o vylepšenie Captcha, založenej na rozoznávaní textu. V oblasti Captcha sme však stále svedkami doťahovania sa vývojárov a útočníkov o to, kto má navrch. No v dnešnej dobe, keď pre útočníka nie je problém zaplatiť ľudí na Východe, ktorí za cent na hodinu ťukajú riešenia Captcha (teda hoci Captcha rieši človek, všetok ostatný proces je, alebo môže byť automatizovaný), je veľmi zložité označiť hocijakú Captcha za neprelomiteľnú.

Vývoj sa však neustále posúva vpred a tak to, čo je dostatočnou ochranou dnes, sa už zajtra môže stať zastaranou technológiou. Môže to zájsť až do fázy, kedy bude text v Captcha natoľko deformovaný, že bude rovnako nečitateľný pre počítač ako aj pre človeka. Keď bude technológia OCR schopná rozoznávať deformovaný text lepšie ako priemerný človek, bude v podstate nepoužiteľná; paradoxne takto však pomáha v rozvoji umelej inteligencie.

Táto práca nezahŕňa všetky existujúce typy Captcha, rovnako ani útoky či vlastnosti, ktoré by mali spĺňať. Nevenovali sme sa všetkému, čo je pre ďalší vývoj Captcha dôležité. Jedná sa o nie starú technológiu a o to rýchlejšie sa vyvíja a mení. Vzniká tak priestor pre budúci výskum v tejto oblasti, napríklad so zameraním na vytvorenie univerzálnej Captcha, príp. užívateľsky čo najpríjemnejšej Captcha ale so zreteľom na bezpečnosť.

# Literatúra


[1] **ALMAZYAD, A.S.; AHMAD, Y.; KOUCHAY, S.A.**: *Multi-Modal CAPTCHA: A User Verification Scheme*. In: Information Science and Applications (ICISA), 2011 International Conference, s.1-7. 2011 [cit. 2013-04-16]. Dostupné z: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5772421&isnumber=5772305

[2] **KADLEC, T.**: *Death to Captchas*. In: TimKadlec.com [online]. 2011 [cit. 2013-04-16]. Dostupné z: http://timkadlec.com/2011/01/death-to-captchas/

[3] **VON AHN, L.; BLUM, M.; HOPPER, N. J.; LANGFORD J.**: *CAPTCHA: Using Hard AI Problems For Security*. In: Advances in Cryptology - Eurocrypt 2003 [online]. 2003 [cit. 2013-03-13]. ISSN 0302-9743. Dostupné z: http://www.captcha.net/captcha_crypt.pdf

[4] **MABEL, J.J.; SUDHA, L.; AARTHY, D.K.; ARSHEY,M.**: *Prevention from online attacks: Captcha, a defensive strategy*. In International Journal of Computer Science and Management Research, Vol 2 Issue 3 March 2013, ISSN 2278-733X. 2003 [cit. 2013-04-13]. Dostupné z: http://www.ijcsmr.org/vol2issue3/paper291.pdf

[5] **HERNANDEZ-CASTRO, C.J.; RIBAGORDA, A.**: *Pitfalls in CAPTCHA design and implementation: The Math CAPTCHA, a case study*, Computers & Security, Volume 29, Issue 1, February 2010, s. 141-157, ISSN 0167-4048, 2003 [cit. 2013-03-10]. Dostupné z: http://www.sciencedirect.com/science/article/pii/S0167404809000728

[6] **Pape, CH.**: *Alternative Authentifizierungsverfahren: Passfaces und CAPTCHAs*. Seminár "Verlässliche Verteilte Systeme", zimný semester 2005/2006, RWTH Aachen. [cit. 2013-03-10] Dostupné z: http://www.fim.uni-linz.ac.at/Lva/SE_Netzwerke_und_Sicherheit_Security_Considerations_in_Intercon_Networks/semA.pdf

[7] **ALSUHIBANY, S.A.**: *Optimising CAPTCHA Generation*. 2011. In: Availability, Reliability and Security (ARES), 2011 Sixth International Conference, pp.740-745. [cit. 2013-03-08] Dostupné z: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6046030&isnumber=6045921

[8] **PENNINGER, S.; MEIER, S.; FEDERRATH, S.**: *Usability von CAPTCHA-Systemen.* 2012. In: GI Sicherheit 2012, 07.-09.03.2012, Darmstadt. [cit. 2013-02-18] Dostupné z: http://epub.uni-regensburg.de/23565/1/CAPTCHA-Usability.pdf

[9] *Ergonomic requirements for Office work with visual display terminal – part 11: Guidance on usability*. 1998. ISO 9241-11:1998 Norm. [cit. 2013-03-27] Dostupné z: http://down.40777.cn/stardard/11/BS%20EN%20ISO%2013406-11999%20Ergonomic%20requirements%20for%20work%20with%20visual%20display%20based%20on%20flat%20panels-Part%201Introduction.pdf

[10] **NAOR, M.**: *Verification of a human in the loop or Identification via the Turing Test*. [online]. 1996 [cit. 2013-03-13]. Dostupné z: http://www.wisdom.weizmann.ac.il/~naor/PAPERS/human.pdf

[11] **MIKLICA, T.**: *CAPTCHA – past na roboty, ale také lidi* [online]. 2011 [cit. 2013-04-16]. Dostupné z: http://www.cnews.cz/captcha-past-na-roboty

[12] **NGUYEN, V.D.; CHOW, Y.-W.; SUSILO, W.**: *Breaking an animated CAPTCHA scheme.*2012. In Proceedings of the 10th international conference on Applied Cryptography and Network Security (ACNS'12). [cit. 2013-02-25] Dostupné z: http://dx.doi.org/10.1007/978-3-642-31284-7_2

[13] **HAICHANG G.; HONGGANG LIU, D.Y.; LIU, X.; WANG, L.**:*A Novel Image Based CAPTCHA Using Jigsaw Puzzle*. 2010. In: 13th IEEE International Conference on Computational Science and Engineering, pp. 351-356, 2010 13th IEEE International Conference on Computational Science and Engineering, 2010. [cit. 2013-02-27]

[14] **RICE, A.**: *A Continued Commitment to Security*. In: Facebook blog [online]. 2011 [cit. 2013-04-16]. Dostupné z: https://blog.facebook.com/blog.php?post=486790652130

[15] **BUSHELL, D.**: *In Search Of The Perfect CAPTCHA*. In: Smashing magazine [online]. 2011 [cit. 2013-04-16]. Dostupné z: http://coding.smashingmagazine.com/2011/03/04/in-search-of-the-perfect-captcha/

[16] **WILKINS, J.**: *Strong CAPTCHA Guidelines v1.2* [online]. 2009 [cit. 2013-03-19]. Dostupné z: http://www.bitland.net/captcha.pdf

[17] *Česká pravidla přístupnosti*. In: Přístupnost.cz - otevřete svůj web všem! [online]. 2006 [cit. 2013-04-16]. Dostupné z: http://www.pristupnost.cz/ceska-pravidla-pristupnosti/

[18] *Chyby typu I a II*. In: Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 5. 4. 2013 [cit. 2013-04-16]. Dostupné z: http://cs.wikipedia.org/wiki/Chyby_typu_I_a_II

[19] **MORI, G.; MALIK, J.**: *Recognizing objects in adversarial clutter: Breaking a visual captcha*. 2003. [cit. 2013-03-25] Dostupné z: http://www.cs.sfu.ca/~mori/research/papers/mori_cvpr03.pdf

[20] **CHELLAPILLA, K.; SIMARD, P.Y.**: *Using machine learning to break visual human interaction proofs (hips)*. 2005. [cit. 2013-03-26] Dostupné z: http://research.microsoft.com/~kumarc/pubs/chellapilla_nips04.pdf

[21] **SKALKA, J.; KLIMEŠ, C.; LOVÁSZOVÁ, G.; ŠVEC, P.** *Informatika na maturity a prijímacie skúšky*. Nitra: Enigma, 2007. ISBN 978-80-89132-50-8.

[22] **RAPAPORT, J. W.**: *The Turing Test* [online]. 2005 [cit. 2013-03-25] Dostupné z: http://www.cse.buffalo.edu/~rapaport/Papers/ell2.pdf

[23] **MORI, G.; MALIK, J.**: *Breaking a Visual CAPTCHA.* In: Greg Mori [online]. 2003 [cit. 2013-04-09]. Dostupné z: http://www.cs.sfu.ca/~mori/research/gimpy/

[24] *Nucaptcha II: Most secure and usable Captcha* [online]. 2011 [cit. 2013-05-09]. Dostupné z: http://www.nucaptcha.com/home

[25] **VAŠKO, R.**: *CAPTCHA: Rozpoznávanie ľudí a počítačov na webe*. Bratislava, 2008. Bakalárska práca. Univerzita Komenského v Bratislave. Vedúci práce RNDr. Richard Ostertág.

[26] *CAPTCHA: HelloCaptcha.com* [online]. 2013 [cit. 2013-05-09]. Dostupné z: http://hellocaptcha.com/

[27] *Was sind CaptchaAds?* [online]. 2009 [cit. 2013-05-09]. Dostupné z: http://www.captchaad.com/startseite/captchaad/was-sind-captchaads/

[28] **Yan, J., El Ahmad, A.S.**: *Captcha Robustness: A Security Engineering Perspective* [online]. In Computer , vol.44, no.2, s.54-60, 2011. [cit. 2013-05-09] Dostupné z: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5601666&isnumber=5713288