Obsah

1 Úvod

Právě sledujeme trend klesání důvěry v tradiční média.

Díky rozšíření Internetu si poprvé v historii mohou lidé po celém světě vyměňovat informace přímo mezi sebou, bez nutnosti centrální instituce. Vzniká tak prostor pro pluralitu názorů, kdy můžeme vidět několik různých (často protichůdných) výkladů též situace, ze kterých lidé vybírají na základě sentimentu, ne objektivního posouzení informace.

Další aktuální trend je pokrok v možnostech úpravy audiovizuálního záznamu a klesající cena potřebných technologií, díky tomu je snazší věrohodně falšovat důkazy o událostech a předpokládám, že v budoucnu pouhý audiovizuální záznam neobstojí jako věrohodný zdroj informací.

Protože kvalitní informovanost je předpoklad k funkční demokratické společnosti, předkládám zde návrh sociální sítě, která vyvíjí tlak na ověřování informací a u každé zprávy zobrazuje její důvěryhodnost pro konkrétního uživatele. Pomocí technologií jako jsou asymetrická kryptografie, peer-to-peer sítě, elektronický podpis a síť důvěry se snažím přenést vztahy fungující v malých lidských skupinách na co největší počet lidí.

2 Problém

V demokratické společnosti hrají sdělovací prostředky (média) zásadní roli, podle Netanela mají tři funkce: 1. kontrolovat, 2. usnadnit veřejnou diskuzi, 3. poskytovat důvěryhodné informace (Netanel, 2001). Protože je demokracie ze své podstaty založena na rozhodování občanů, je třetí bod velmi důležitý pro celou společnost. Tradiční média tento úkol plnily po staletí, ale nyní důvěra v ně postupně klesá.

Mohlo by se zdát, že televize je nejdůvěryhodnější zdroj informací - dokáže přenést obraz i zvuk a divák pozná, jestli záznam mluvícího člověka na obrazovce je věrohodný nebo ne. Ale s pokrokem v možnostech úpravy audiovizuálního záznamu a s klesáním ceny k tomu potřebných technologií (podle Moorova zákona se výkon polovodičových součástek zdvojnásobí přibližně každé dva roky při zachování ceny (Moore, 2004)[1]) toto platit přestává. Příklady jsou následující: Společnost *Adobe* představila nástroj na úpravu hlasového záznamu, kterému stačí vzorek něčího hlasu a posléze je schopný syntetizovat jakékoliv vyjádření (Anthony, 2016). Ve filmu *Rogue One* ze série *Star Wars* vystupovaly postavy, jejichž herci byly v době natáčení po smrti, nebo výrazně viditelně starší (Cooper, 2017). Thies et al. navrhli program, který v reálném času umožňuje velmi věrohodně zaměnit výraz člověka ve videu podle výrazu herce snímaného kamerou (Thies et al., 2016).

Další z problémů s tradičními médii je tzv. *gatekeeping* - média jsou zpravidla centrálně řízené organizace s hierarchickou strukturou, informace postupně prochází přes několik instancí v této struktuře a při každém kroku jsou posuzovány a upravovány (Dragoni et al., 2013). Tímto proces je zajištěna důvěryhodnost a kvalita informací, ale to znamená, že pro jednotlivce je příliš snadné informaci poškodit (ať už úmyslné, či omylem).

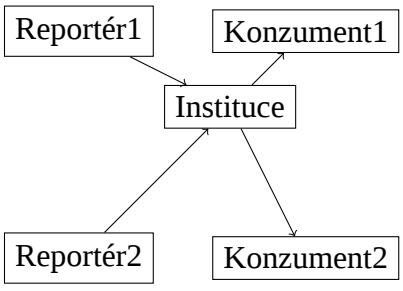
Podle Dragoni et al. je tento tok informací jednosměrný a koncový konzument nemá možnost jak v reálném čase podat zpětnou vazbu, proto vzniká problém zvaný *agenda-setting*, kdy téma veřejné debaty určují média (Dragoni et al., 2013). Koncový konzument ale může začít konzumovat jiné médium a tak jej může ovlivnit prostřednictví volného trhu.

Klesání důvěry v tradiční média potvrzují např. Janda; Blažejovská et al., když říkají, že 25.5% Čechů věří alternativním médiím[2] a 24.5% Čechů jim věří více než tradičním médiím[3] (Janda; Blažejovská et al., 2016). Tyto média přitom šíří úplně nebo částečně nepravdivé informace, které často zpochybňují demokratické instituce a pozitivně se vyjadřují k režimům s vetší, či

[1] Původně každý rok (Moore, 1965), ale v roce 1975 upraveno a tak je zákon platný dodnes.

[2] Například Parlamentní listy, AC24.cz, PrvníZprávy.cz

[3] Například Česká televize, Český rozhlas či deníky Právo nebo Hospodářské noviny



Obrázek 2.1: Centralizované médium

menší mírou nesvobody (Janda; Víchová, 2016). Navíc se jim tento styl uvažování daří šířit společností (Janda; Blažejovská et al., 2016).

Problém popsaný v této kapitole vede k paradoxnímu vztahu, kdy s technickým pokrokem stoupá hodnota očitého svědectví.

3 Řešení

Protože není v silách jednotlivce byt očitým svědkem všech událostí ovlivňujících jeho rozhodování, potřebujeme nový systém distribuce a sběru zpráv, které nebude trpět neduhy popsanými v kapitole 2.

Často zaklínaným řešením je prostá peer-to-peer síť (Twitter, Facebook, ...), kde si každý může publikovat cokoliv, tyto sítě ale trpí nedostatkem sebekontroly a stávají se prostorem pro šíření různých falešných zpráv (Netanel, 2001). Proto například Giasemidis et al. navrhují systém, který určí důvěryhodnost těchto informací (Giasemidis et al., 2016), nebo Mishra et al. kteří popisují různé metody detekce manipulovaní s obrazem (Mishra et al., 2013). Zde navržený systém je podobný Dragoni et al., ale přidávám osobní reputaci uživatele, kterou se zaručuje za každý svůj krok a tato reputace zároveň ovlivňuje váhu každého kroku, tímto je vyvíjen tlak na to, aby se uživatel choval zodpovědně.

3.1 Zpráva

Zprávou se myslí informace o nějaké události, které byl uživatel zprávu publikující očitým svědkem - může se osobně zaručit za její pravdivost.

Zpráva obsahuje místo, kterého se týká (přesnost tohoto určení je ponechána na uživateli), samotný text zprávy a případnou obrazovou či zvukovou dokumentaci.

Každá zpráva je podepsána uživatelem, který ji publikoval (použije svůj soukromý klíč) a ten se tím osobně zaručuje za její pravost. Zprávu poté dále podepisují uživatelé, kteří se také mohou osobně zaručit za její pravost, zároveň se mohou zaručit za její nepravost. Pokud je počet uživatelů, kteří se zaručili za pravost zprávy (podepsali ji) menší, než počet uživatelů, kteří se zaručili za její nepravost, je zpráva označena jako nepravdivá, uživateli, který ji publikoval (původní uživatel) a všem kteří ji garantovali jako pravou (sekundární uživatelé) je snížena reputace (dost výrazně na to, aby si nedovolili toto opakovat). Pokud se zpráva ukáže jako pravá (počet uživatelů, kteří ji potvrdili bude větší, než počet uživatelů, kteří ji zamítli) reputace původního a sekundárních uživatelů se zvýší.

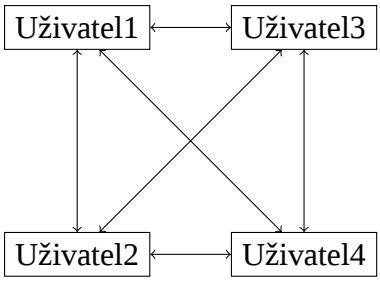
3.2 Decentralizace

Odstraněním centrální instituce sice zmizí problémy popisované v kapitole 2, ale zároveň se garance kvality informace přesune z instituce dávající všanc svojí reputaci na jednotlivce, který si kdykoliv může založit jiný účet pod jinou identitou. Navíc bychom sami museli prohlédnout všechny informace a rozhodnout zda jsou pro nás relevantní, což také není v silách jednotlivce. (Netanel, 2001)

Zbavit se centrální instituce je žádoucí, ale potřebujeme jiný mechanismus jak zaručit původ a důvěryhodnost zprávy a mechanismus, který bude zprávy filtrovat.

3.3 Uživatel

V decentralizovaném systému je uživatel základní jednotkou, má čtyři role: 1. publikovat zprávy, 2. přijímat zprávy, 3. validovat zprávy a za 4. validovat uživatele. Jeho hlavními atributy jsou certifikát a reputace.



Obrázek 3.1: Decentralizované médium, obyčejná peer-to-peer síť

Certifikát uživatele se obsahuje identitu uživatele, (jméno, e-mailová adresa, číslo občanského průkazu, adresa bydliště, ...) podle které je jednoznačně možné ho identifikovat, veřejný klíč, podpisy ostatních uživatelů a jeho reputaci jakožto validátora uživatelů (rozdílná od reputace jakožto vydavatele zpráv).

3.4 Síť důvěry

Protože je potřeba zajistit pravost identity uživatele, ostatní uživatelé se mohou osobně zaručit za jeho pravost svojí reputací podepsáním jeho certifikátu (validací), můžeme si to představit jako potvrzení přátelství na sociální síti Facebook (Network Associates, 1999).

Tímto se buduje síť důvěry a díky tomu je možné zjistit vzdálenost uživatelů, tedy kolik uživatelů je potřeba propojit, aby se spojili dva uživatelé, toto číslo je průměrně šest (Network Associates, 1999).

Z pohledu uživatele (Alice) závisí důvěryhodnost jiného uživatele (Boba) na bobově reputaci, vzdálenosti Alice od Boba, kolik uživatelů podepsalo bobův certifikát a důvěryhodnosti těchto uživatelů vzhledem k Alici.

Uživatele je potřeba motivovat k pečlivému ověření identity před validací uživatele, aby nedocházelo ke vzniku falešných uživatelů, ve skutečnosti neexistujících. To zajišťuje mechanismus, který v případě, že se uživatel ukáže jako falešný sníží důvěryhodnost všem uživatelů, kteří podepsali jeho certifikát a tím pádem se sníží důvěryhodnost všech uživatelů, kterým tito uživatelé podepsaly certifikát.

Tato síť by měla být nezávislá na systému distribuce zpráv a měla by být kompatibilní se systémem PGP.

Detailní návrh sítě důvěry by vydal na celou další práci a hodlám se jím zabývat při implementaci celého systému.

3.5 Příjem zprávy

Při příjmu (zobrazení) zprávy se uživateli (Alici) zobrazí obsah zprávy a důvěryhodnost konkrétní zprávy pro konkrétního uživatele. Alice má možnost zprávu potvrdit nebo zamítnout.

Důvěryhodnost zprávy závisí na vzdálenosti původního uživatele od Alice, reputaci původního uživatele, počtu a vzdálenosti sekundárních uživatelů od Alice a jejich reputaci. Samotné rozhodnutí, zda je zpráva pravdivá nebo ne je ponecháno na Alici, i když existují pokusy o automatizaci tohoto rozhodnutí (např. Giasemidis et al., 2016), kategoricky jsem se rozhodl nechat toto rozhodnutí na uživateli.

3.6 Nevýhody

Jedno ze slabých míst je předpoklad, že si uživatel (zdroj informace) může dovolit zveřejnit svou identitu, což často v represivních režimech není slučitelné s přežitím. Také je nutné dosáhnout určitého množství uživatelů, aby síť začala být užitečná. Jinak nebude dostatek zdrojů informací a dostatek uživatelů, kteří budou svědky jedné události

4 Závěr

V práci jsem popsal problém tradičních médií (klesající důvěryhodnost), proč nás tento problém trápí (nefungující demokracie) a navrhl řešení, které se snaží tyto problémy vyřešit.

Návrhem je sociální síť, kde zdrojem zpráv jsou sami její uživatelé, ale na rozdíl od většiny takto navržených sítí (Facebook, Twitter, ...) zprávy jsou garantovány osobní reputací uživatelů.V praxi by si tak nikdo neměl dovolit zveřejnit zprávu za kterou se nemůže zaručit a když už se taková věc stane, zpráva by měla být zavržena ostatními uživateli.

Protože by bylo naivní spoléhat na to, že se uživatelé budou chovat zodpovědně, je síť navržena tak, aby vedla uživatele k zodpovědnému chování, pomocí osobní reputace uživatelů.

Používání takového systému si představuji tak, že vznikne mobilní aplikace, ze které budou uživatelé publikovat a přijímat zprávy. Aplikaci budou používat například na zasedání lokálních zastupitelství, v galerii poslanecké sněmovny nebo prostě když budou svědkem události, která jim přijde významná.

Ostatní uživatelé pak dodají zprávě na důvěryhodnosti a významu, nebo zpráva zapadne, toto se bude dít přirozenou cestou, bez potřeby centrální instituce. I úložiště zpráv a certifikátů uživatelů by mělo být distribuované (například pomocí *Interplanetary File System*[1], Benet, 2014.).

Mojí další činností bude implementovat zde navržený systém a postarat se o jeho rozšíření, pokud se ukáže jako životaschopný.

[1]Meziplanetární souborový systém, navržený s důrazem na zachování integrity dat a jejich distribuovanému rozložení

Slovník

asymetrická kryptografie Šifrování pomocí veřejných a soukromých klíčů, nevyžaduje sdílené tajemství (např. heslo) (Menezes et al., 1996, str. 25). 4

elektronický podpis Mechanismus, pomocí kterého můžeme ověřit, že zpráva opravdu pochází od uživatele, který ji podepsal (Menezes et al., 1996, str. 22). 4

peer-to-peer Decentralizovaná síť, kde jsou jednotlivé uzly propojeny přímo mezi sebou. 4, 7, 8

PGP *Pretty Good Privacy*, oblíbený systém pro šifrované přenášení zpráv pomocí asymetrické kryptografie, viz. Callas et al., 2007; Network Associates, 1999. 8

soukromý klíč Klíč pomocí kterého odesílatel zašifruje zprávu, musí být známý jenom odesílateli (Menezes et al., 1996, str. 29) (v této práci). 7

tradiční média Zde myšlen tisk, televize a rozhlas.. 4, 5

veřejný klíč Klíč odesílatele pomocí kterého příjemce dešifruje zprávu, ověří její původ od odesílatele (Menezes et al., 1996, str. 29) (v této práci). 8

Bibliografie

ANTHONY, Sebastian, 2016. *Adobe demos "photoshop for audio," lets you edit speech as easily as text* [online] [cit. 2017-02-23]. Dostupné z: http://web.archive.org/web/20170223084757/https://arstechnica.co.uk/information-%20technology/2016/11/adobe-voco-photoshop-for-audio-speech-editing/.

BENET, Juan, 2014. IPFS-content addressed, versioned, P2P file system. *arXiv preprint arXiv:1407.3561*.

CALLAS, Jon; DONNERHACKE, Lutz; FINNEY, Hal; SHAW, David; THAYER, Rodney, 2007. *OpenPGP Message Format* [Internet Requests for Comments]. RFC Editor. Dostupné také z: https://tools.ietf.org/pdf/rfc4880.pdf. RFC. RFC Editor.

COOPER, Gael Fashingbauer, 2017. *Watch how 'Rogue One' brought back young Princess Leia, Tarkin* [online] [cit. 2017-01-08]. Dostupné z: http://web.archive.org/web/20170108193444/https://www.cnet.com/news/rogue-one-star-wars-story-cgi-young-princess-leia-tarkin/.

DRAGONI, Manuel Mazzara Nicola; MARRAFI'A, Luca Biselli Antonio; NICOLA, Simona de, 2013. Social networks and collective intelligence: A return to the Agora. *Social Network Engineering for Secure Web Data and Services*, s. 88.

GIASEMIDIS, Georgios; SINGLETON, Colin; AGRAFIOTIS, Ioannis; NURSE, Jason RC; PILGRIM, Alan; WILLIS, Chris; GREETHAM, Danica Vukadinovic, 2016. Determining the veracity of rumours on Twitter. In: *Determining the veracity of rumours on Twitter*. *International Conference on Social Informatics*, s. 185–205.

JANDA, Jakub; BLAŽEJOVSKÁ, Markéta; VLASÁK, Jakub, 2016. *Dopady dezinformačních operací v České republice*. Dostupné také z: http://www.evropskehodnoty.cz/wp-content/uploads/2016/09/Dopady-dezinforma%C4%8Dn%C3%ADch-operac%C3%AD-v-%C4%8Cesk%C3%A9-republice.pdf. Evropské hodnoty z.s.

JANDA, Jakub; VÍCHOVÁ, Veronika, 2016. *Fungování českých dezinformačních webů*. Dostupné také z: http://www.evropskehodnoty.cz/wp-content/uploads/2016/07/Fungov%C3%A1n%C3%AD-%C4%8Desk%C3%BDch-dezinforma%C4%8Dn%C3%ADch-web%C5%AF_F.pdf. Evropské hodnoty z.s.

MENEZES, Alfred J.; OORSCHOT, Paul C. van; VANSTONE, Scott A., 1996. *Handbook of Applied Cryptography*. Boca Raton: CRC Press. ISBN 978-0-8493-8523-0.

MISHRA, Minati; ADHIKARY, M. C., 2013. Digital Image Tamper Detection Techniques - A Comprehensive Study. *International Journal of Computer Science and Business Informatics*. Roč. 2, č. 1. ISSN 1694-2108.

MOORE, Gordon E., 1965. Cramming more components onto integrated circuits. *Electronics*. Roč. 38, č. 8.

MOORE, Gordon E., 2004. Progress in digital integrated electronics. *SPIE MILESTONE SERIES MS*. Roč. 178, s. 179–181.

NETANEL, Neil, 2001. Is the Comercial Mass Media Secessary, or Even Desirable, for Liberal Democracy? *arXiv preprint cs/0109092*.

NETWORK ASSOCIATES, Inc., 1999. *An Introduction to Cryptography*. Dostupné také z: ftp://ftp.pgpi.org/pub/pgp/6.5/docs/english/IntroToCrypto.pdf.

THIES, J.; ZOLLHÖFER, M.; STAMMINGER, M.; THEOBALT, C.; NIEßNER, M., 2016. Face2Face: Real-time Face Capture and Reenactment of RGB Videos. In: *Face2Face: Real-time Face Capture and Reenactment of RGB Videos*. *Proc. Computer Vision and Pattern Recognition (CVPR), IEEE*.