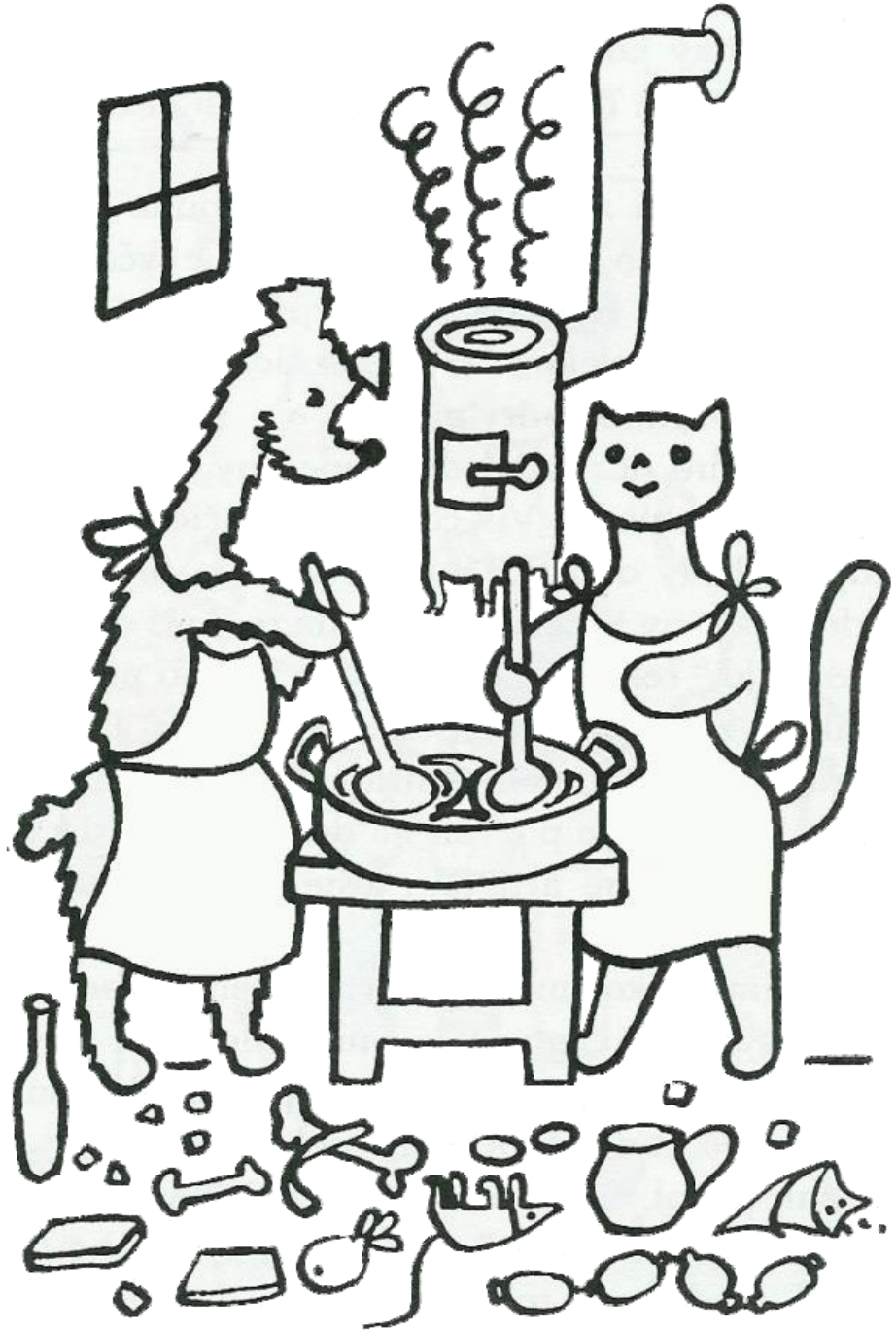
Nástroje a možnosti internetu

Internet jako nástroj sledování II.

5. 11. 2021



Vyzkoušeli jste některé z nástrojů zmíněných minule?

HTTPS

HTTPS

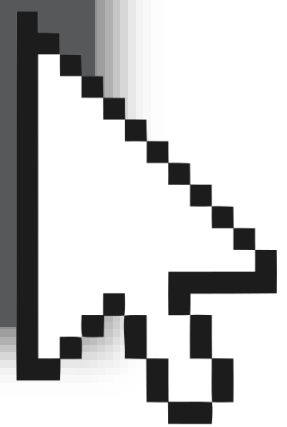
- co je za potíže s HTTP?
- SSL a certifikace
- šifrované propojení
- HTTPS Everywhere

Vyhláška č. 357/2012 Sb. o uchovávání, předávání a likvidaci provozních a lokalizačních údajů

Program

SOBOTA - 6. LISTOPAD

TRACK 2	TRACK 3	TRACK 4	
orek: Jak vzniká junior.guru: Výdělečný artup“ v jednom člověku	**Jan Vobořil, Jan Cibulka:** Data retention - nekonečný příběh plošného šmírování	**Štěpán Bechynský:** Úvod do Node-RED	
aja: Zaměřeno na budoucnost Internetu	**Michal Konečný:** Jak se rozloučit s Googlem	**Pavel Píša, Michal Lenc:** Otevřený návrh řídicích aplikací s pysimCoder a NuttX	



HTTPS

- **ALE...**
- metadata jako velmi cenný vhled

```
[2020/11/19 17:30] google.cz
[2020/11/19 17:33] hnutiprozivot.cz
[2020/11/19 17:37] potrat.cz
[2020/11/19 17:39] napocatku.cz
[2020/11/19 17:44] fnbrno.cz
[2020/11/19 18:01] mapy.cz
```

HTTPS

- **ALE…**
- *website fingerprinting*
  identifikace jednotlivých stránek
- odhadování *query* podle množství dat

2012 IEEE Symposium on Security and Privacy

Peek-a-Boo, I Still See You:
Why Efficient Traffic Analysis Countermeasures Fail

Kevin P. Dyer*, Scott E. Coull†, Thomas Ristenpart‡, and Thomas Shrimpton*

*Department of Computer Science, Portland State University, Portland, USA. Email: {kdyer, teshrim}@cs.pdx.edu
† RedJack, LLC., Silver Spring, MD, USA Email: scott.coull@redjack.com
‡Department of Computer Sciences, University of Wisconsin-Madison, USA. Email: rist@cs.wisc.edu

RESEARCH-ARTICLE

Touching from a distance: website fingerprinting attacks and defenses

Authors: Xiang Cai, Xin Cheng Zhang, Brijesh Joshi, Rob Johnson Authors Info & Affiliations

Publication: CCS '12: Proceedings of the 2012 ACM conference on Computer and communications security • October 2012 • Pages 605–616 • https://doi.org/10.1145/2382196.2382260

112 1,216 Get Access

ABSTRACT

We present a novel web page fingerprinting attack that is able to defeat several recently proposed defenses against traffic analysis attacks, including the application-level defenses HTTPOS and randomized pipelining over Tor. Regardless of the defense scheme, our attack was able to guess which of 100 web pages a victim was visiting at least 50% of the time and, with some defenses, over 90% of the time. Our attack is based on a simple model of network behavior and out-performs previously proposed ad hoc attacks. We then build a web site fingerprinting attack that is able to identify whether a victim is visiting a particular web site with over 90% accuracy in our experiments.

VPN

VPN

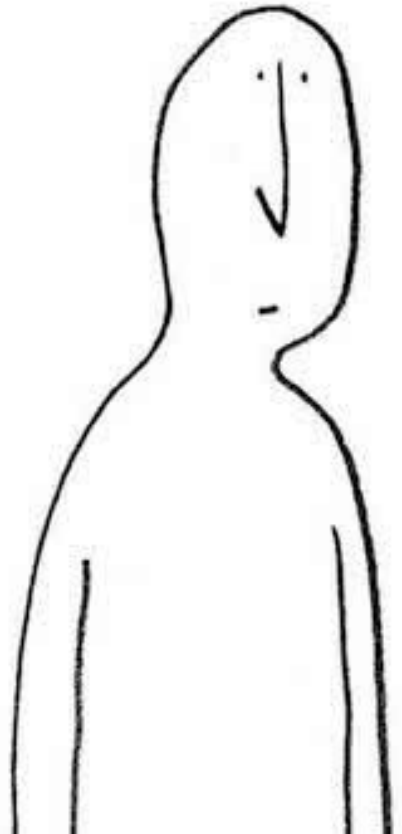
- důležitým identifikátorem je IP adresa
- *virtuální privátní síť* – k čemu to je?

- jaké to má potíže?
- zdarma = pomalé a *no*-no-log policy
- malá adopce pro běžné užití
- přenášení důvěry *(ISP -> VPN poskytovatel)*
- *cookies?* – není to buď/nebo…

Jak to mám já?

- placená VPN
- hostováno ve Švýcarsku
- transparentnost
- *dvousečná zbraň*

January 2019 – A data request from a foreign country was approved by the Swiss court system. However, as we do not have any customer IP information, we could not provide the requested information and this was explained to the requesting party.



Platformy

Náš obsah leží jinde

- *Gmail, Facebook,...*
- přístup k vlastním datům?
- kontrola nad daty?
- nastavení soukromí?
- **data leaks / breach**
- have i been pwned?

Instagram bug could have allowed others to read your direct messages

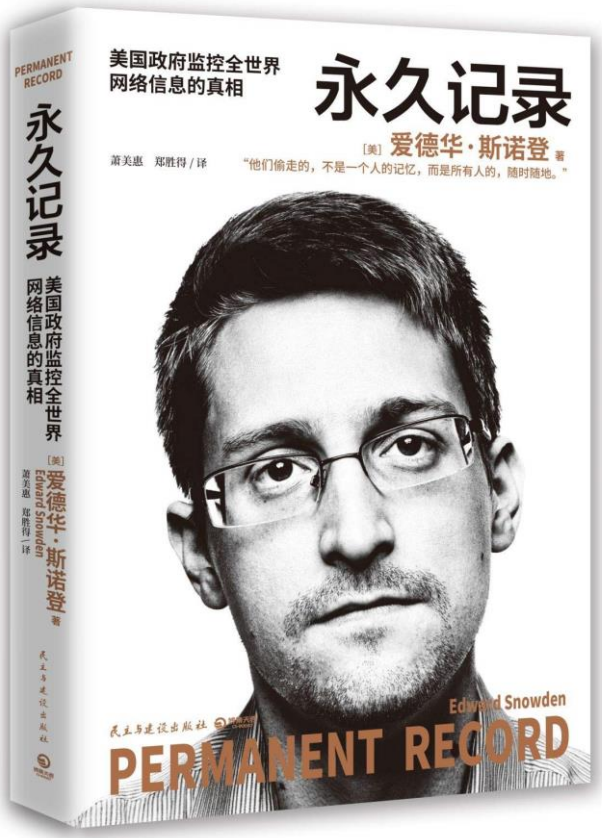
17 FEB 2016 3

Privacy, Social networks

Previous: "Locky" ransomware – what you need to know

Next: Apple says NO to iPhone backdoor in terror case

backdoor


PERMANENT RECORD
永久记录
美国政府监控全世界网络信息的真相
[美]爱德华·斯诺登 著
萧美惠 郑胜得 / 译
"他们偷走的，不是一个人的记忆，而是所有人的，随时随地。"
Edward Snowden
PERMANENT RECORD

TOP SECRET//SI//ORCON//NOFORN

PRISM/US-984XN Overview

OR

*The SIGAD Used **Most** in NSA Report*
Overview

[redacted]

April 2013

Derive

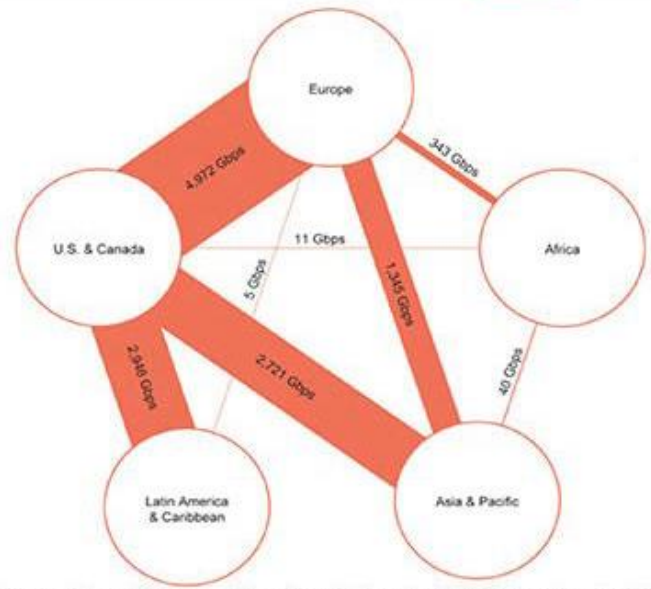
TOP SECRET//S

TOP SECRET//SI//ORCON//NOFORN

(TS//SI//NF) Introduction

U.S. as World's Telecommunications Backbone

- Much of the world's communications flow through the U.S.
- A target's phone call, e-mail or chat will take the **cheapest** path, **not the physically most direct** path – you can't always predict the path.
- Your target's communications could easily be flowing into and through the U.S.



International Internet Regional Bandwidth Capacity in 2011
Source: Telegeography Research

TOP SECRET//SI//ORCON//NOFORN

TOP SECRET//SI//ORCON//NOFORN

(TS//SI//NF) FAA702 Operations

Two Types of Collection

Upstream

- Collection of communications on fiber cables and infrastructure as data flows past.

(FAIRVIEW, STORMBREW, BLARNEY, OAKSTAR)

You Should Use Both

PRISM

- Collection directly from the servers of these U.S. Service Providers: Microsoft, Yahoo, Google Facebook, PalTalk, AOL, Skype, YouTube Apple.

TOP SECRET//SI//ORC

TOP SECRET//SI//ORCON//NOFORN

(TS//SI//NF) PRISM Collection Details

Current Providers

- Microsoft (Hotmail, etc.)
- Google
- Yahoo!
- Facebook
- PalTalk
- YouTube
- Skype
- AOL
- Apple

What Will You Receive in Collection (Surveillance and Stored Comms)?
It varies by provider. In general:

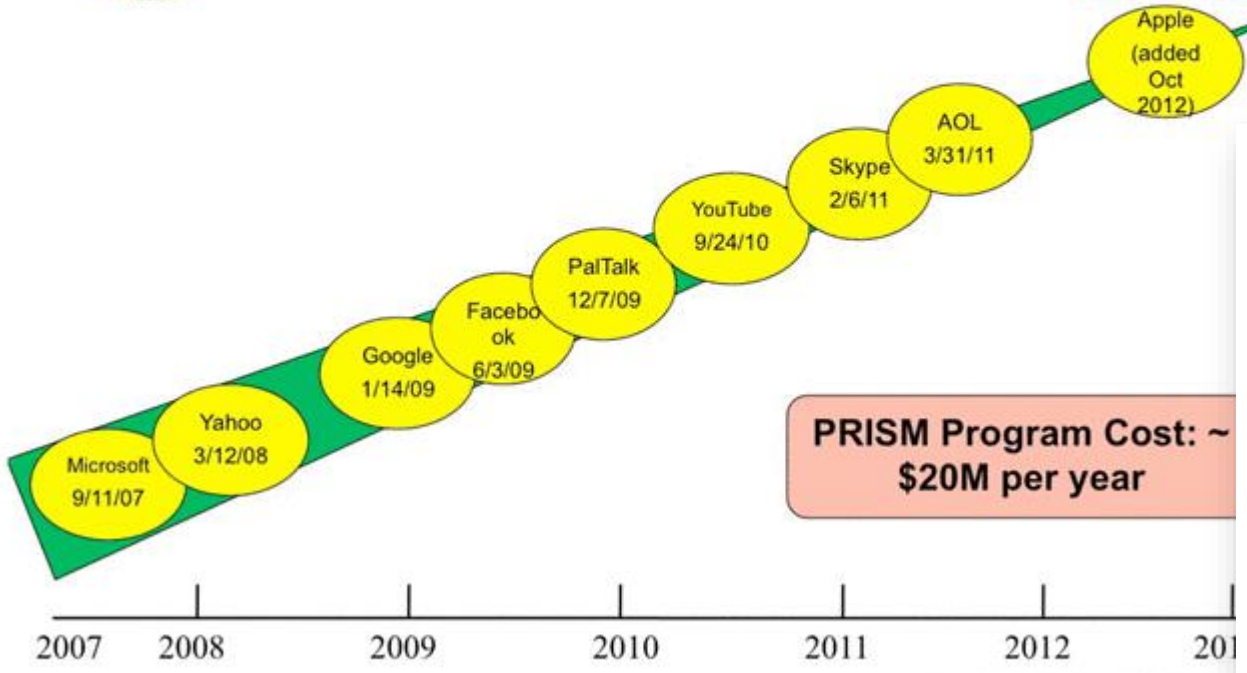
- E-mail
- Chat – video, voice
- Videos
- Photos
- Stored data
- VoIP
- File transfers
- Video Conferencing
- Notifications of target activity – logins, etc.
- Online Social Networking details
- **Special Requests**

Complete list and details on PRISM web page:
Go PRISMFAA

TOP SECRET//SI//ORCON//NOFORN

TOP SECRET//SI//ORCON//NOFORN

(TS//SI//NF) Dates When PRISM Collection Began For Each Provider



TOP SECRET//SI//ORCON//N

TOP SECRET//SI//ORCON//NOFORN

(TS//SI//NF) PRISM Case Notations

P2ESQC120001234

PRISM Provider
- P1: Microsoft
- P2: Yahoo
- P3: Google
- P4: Facebook
- P5: PalTalk
- P6: YouTube
- P7: Skype
- P8: AOL
- PA: Apple

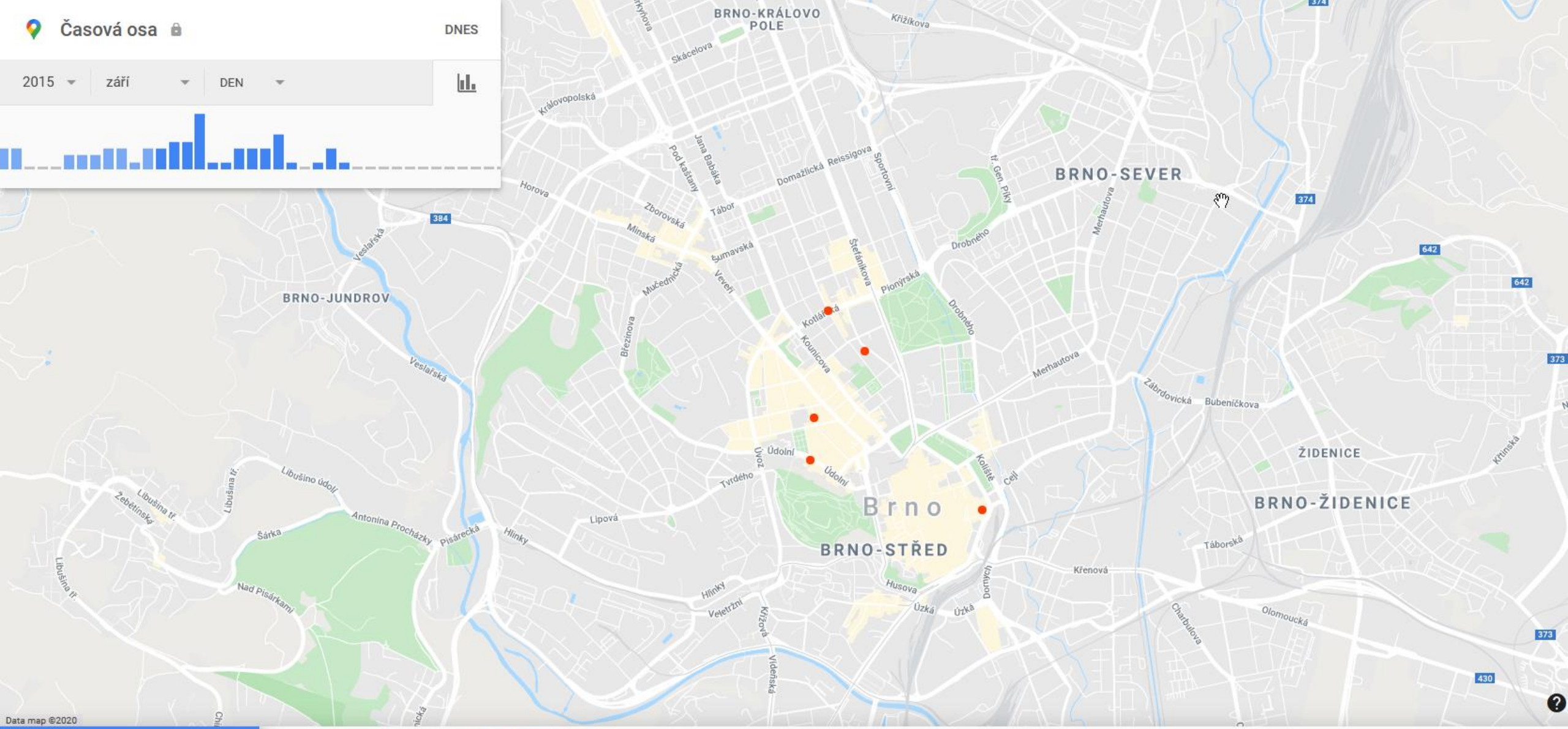
Fixed trigraph, denotes PRISM source collection

Year CASN established for selector

Serial #

Content Type
- A: Stored Comms (Search)
- B: IM (chat)
- C: RTN-EDC (real-time notification of an e-mail event such as a login or sent message)
- D: RTN-IM (real-time notification of a chat login or logout event)
- E: E-Mail
- F: VoIP
- G: Full (WebForum)
- H: OSN Messaging (photos, wallposts, activity, etc.)
- I: OSN Basic Subscriber Info
- J: Videos
- . (dot): Indicates multiple types

TOP SECRET//SI//ORCON//NOFORN



září 2015

1 zajímavé místo

Odpoledne Taneční konzervatoř, Brno, Nejedlého 3

10. 9. 2015

Vyberte možnost automatického mazání pro Historii polohy

- (●) **Automaticky mazat aktivitu starší než 3 měsíce**
  a ručně lze smazat kdykoli
- ( ) **Automaticky mazat aktivitu starší než 18 měsíců**
  a ručně lze smazat kdykoli
- ( ) **Automaticky mazat aktivitu starší než 36 měsíců**
  a ručně lze smazat kdykoli
- ( ) **Nemazat automaticky**

Jak dlouho?

Když uchováváte historii polohy, máte možnost zpětně dohledat navštívená místa i trasy, po kterých jste cestovali. Tato data můžete přestat ukládat pozastavením historie polohy.

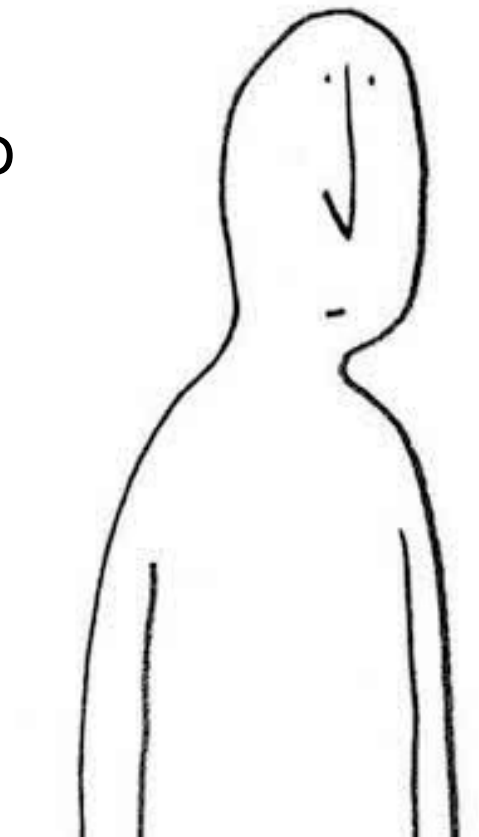
Další

Co se stane po úniku dat?

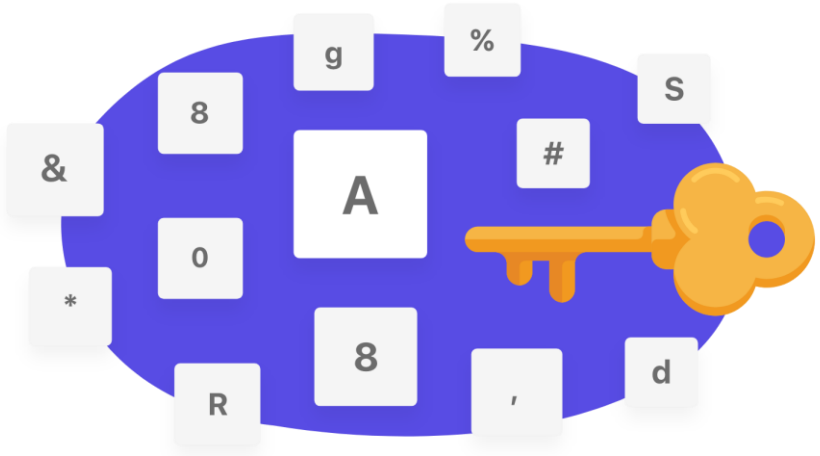
- objeví se to venku
- často náhodně, často až po čase
- mnohdy k zakoupení
- začne se zkoušet, testovat, kombinovat
- ověřuje se pravdivost a aktuálnost
- *hledá se zdroj* – mnohdy kombinace
- reportuje se

Jak to mám já?

- proklikávám všechna nastavení soukromí
- snažím se dočíst, co které znamená
- nastaveny alerty na úniky dat
- po úniku kontroluji, co může být ohroženo



Hesla



- pevná hesla
- správci hesel – jaké to má potíže?
- **2FA** *(knowledge, possession, inherent, location)*
- Leaked Passwords
- slovník / brute force / credential stuffing

Pokud chcete lísteček, nastavte si jasná pravidla!

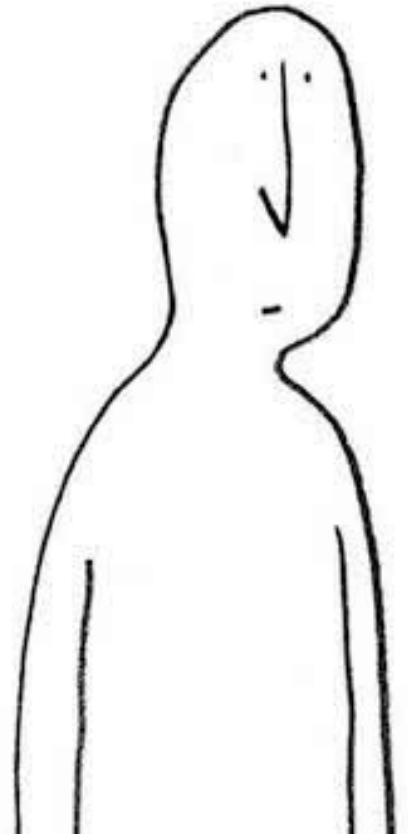

MilFlip Logon Details
ATTENTION ALL CRMS STUDENTS
SCARPA


MilFlip Logon
Details

Jak to mám já?

- LastPass jako správce hesel
- silné unikátní heslo
- některá hesla jen v hlavě
- 2FA skrze HW klíč

	A B C	D E F	G H I	J K L	M N O	P Q R	S T U	V W X	Y Z	
0	h i h	v k g	z u v	p 5 i	g b k	e a e	k t i	f d 6	p 6	0
1	x 6 2	s c b	2 j w	d r p	y e 4	u n c	v y g	w 5 s	g e	1
2	y k c	e i z	c b i	e c c	q z g	7 f 6	d b r	s d e	h k	2
3	3 e 5	b i u	n k z	w d 3	x n 7	z q p	s x n	x u r	y d	3
4	a 4 i	i f d	n b e	x v s	b n f	e g 5	s f w	a u f	x 9	4
5	5 i r	u n r	p w 2	v 2 g	w 6 5	j q 6	y w c	6 s u	c g	5
6	v x m	j w h	u f 4	9 x j	w q 6	p x u	m t 6	4 r v	r t	6
7	s b f	v h 2	j u c	9 4 w	e x w	3 9 k	j 6 z	9 r e	t n	7
8	9 b b	r v u	s 2 g	z t s	m v r	g j w	5 9 r	5 j 3	2 c	8
9	2 i h	m x g	n z x	b k g	3 s 9	m c k	a t s	k h p	j y	9
	A B C	D E F	G H I	J K L	M N O	P Q R	S T U	V W X	Y Z	



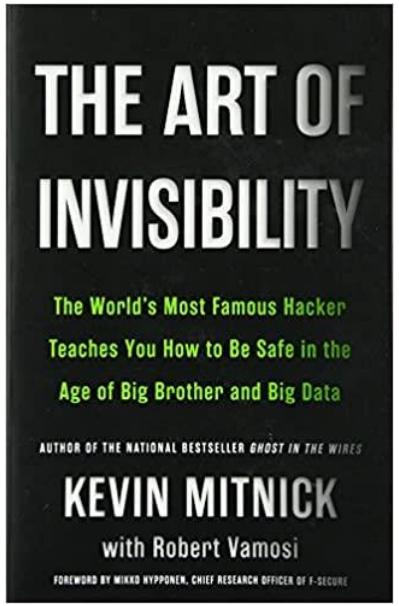
Šifrování

- *end-to-end šifrování*
- WhatsApp, Signal, Threema
- *jaké to má potíže?*
- *kritický počet uživatelů*
- zadní vrátka
- má to kontext!

- *šifrování dat na disku?* – USB flash

Ekosystém

Není to jen o PC



Každé nové zařízení zapadne do ekosystému.

- **mobil** jako vstupní brána do vašeho života
- mobil jako další zdroj dat – *všudypřítomný*
- geolokace

- anonymita? – *burner* – Kevin Mitnick
- IMSI CATCHER – Agáta

Není to jen o PC

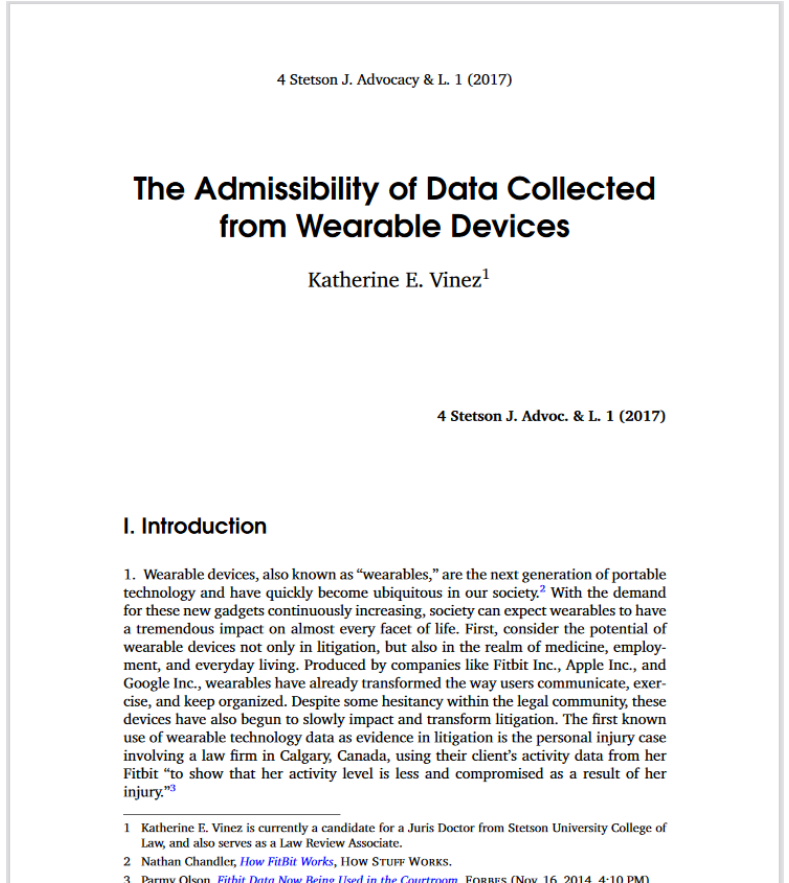
- **IoT** – internet věcí, chytrá zařízení
- IoT jako bezpečnostní problém
- IoT jako zdroj cenných dat - Shodan

- chytrá žárovka

- chytrá města
- anonymizace a deanonymizace

Není to jen o PC

- **wearables**
- nositelné technologie
- *quantified self*



4 Stetson J. Advocacy & L. 1 (2017)

The Admissibility of Data Collected from Wearable Devices

Katherine E. Vinez[1]

4 Stetson J. Advoc. & L. 1 (2017)

I. Introduction

1. Wearable devices, also known as "wearables," are the next generation of portable technology and have quickly become ubiquitous in our society.[2] With the demand for these new gadgets continuously increasing, society can expect wearables to have a tremendous impact on almost every facet of life. First, consider the potential of wearable devices not only in litigation, but also in the realm of medicine, employment, and everyday living. Produced by companies like Fitbit Inc., Apple Inc., and Google Inc., wearables have already transformed the way users communicate, exercise, and keep organized. Despite some hesitancy within the legal community, these devices have also begun to slowly impact and transform litigation. The first known use of wearable technology data as evidence in litigation is the personal injury case involving a law firm in Calgary, Canada, using their client's activity data from her Fitbit "to show that her activity level is less and compromised as a result of her injury."[3]

1 Katherine E. Vinez is currently a candidate for a Juris Doctor from Stetson University College of Law, and also serves as a Law Review Associate.

2 Nathan Chandler, *How FitBit Works*, How Stuff Works.

3 Parmy Olson, *Fitbit Data Now Being Used in the Courtroom*, Forbes (Nov. 16, 2014, 4:10 PM)

Není to jen o PC

- **IVA** - Alexa, Cortana a podobné...
- bezpečnostní problémy

DE GRUYTER OPEN Proceedings on Privacy Enhancing Technologies 2018; 18 (4):1–18

Elleen Pan*, Jingjing Ren, Martina Lindorfer, Christo Wilson, and David Choffnes

Panoptispy: Characterizing Audio and Video Exfiltration from Android Applications

Abstract: The high-fidelity sensors and ubiquitous internet connectivity offered by mobile devices have facilitated an explosion in mobile apps that rely on multimedia features. However, these sensors can also be used in ways that may violate user's expectations and personal privacy. For example, apps have been caught taking pictures without the user's knowledge and passively listened for inaudible, ultrasonic audio beacons. The developers of mobile device operating systems recognize that sensor data is sensitive, but unfortunately existing permission models only mitigate some of the privacy concerns surrounding multimedia data.

In this work, we present the first large-scale empirical study of media permissions and leaks from Android apps, covering 17,260 apps from Google Play, AppChina, Mi.com, and Anzhi. We study the behavior of these apps using a combination of static and dynamic analysis techniques. Our study reveals several alarming privacy risks in the Android app ecosystem, including apps that over-provision their media permissions and apps that share image and video data with other parties in unexpected ways, without user knowledge or consent. We also identify a previously unreported privacy risk that arises from third-party libraries that record and upload screenshots and videos of the screen without informing the user and without requiring any permissions.

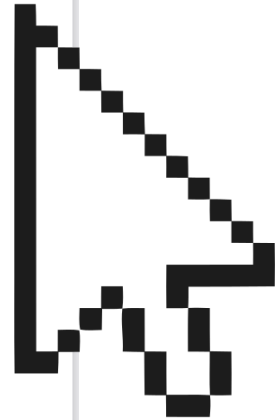
Keywords: privacy; mobile devices; audio, video, and image leaks

1 Introduction

The high-fidelity sensors and ubiquitous internet connectivity offered by mobile devices have facilitated numerous mobile applications (apps) that rely on multimedia features. For example, a mobile device's camera and microphone enable users to capture and share pictures, videos, and recorded audio. Apps also use these sensors to implement important services such as voice assistants, optical character recognition (OCR), music identification, and face and object recognition.

In addition to such beneficial use cases, apps may use these sensors in ways that violate users' expectations and privacy. For example, some apps take pictures without the user's knowledge by shrinking the viewfinder preview window to a 1×1 pixel, thus making it virtually invisible [51, 68]. Similarly, Silverpush, an advertising company, developed a library that passively listened for inaudible, ultrasonic audio beacons for tracking users' TV viewing habits [28]. Finally, as a possible example of things to come, Facebook has been awarded a patent on using the mobile device's camera to analyze users' emotions while they are browsing the newsfeed [70].

Given that sensor data is highly sensitive, the Android and iOS operating systems include mandatory access control mechanisms around most sensors. However, existing permission models only partially mitigate multimedia privacy concerns because they are *coarse grained* and *incomplete*. For example, when a user grants



Není to jen o PC

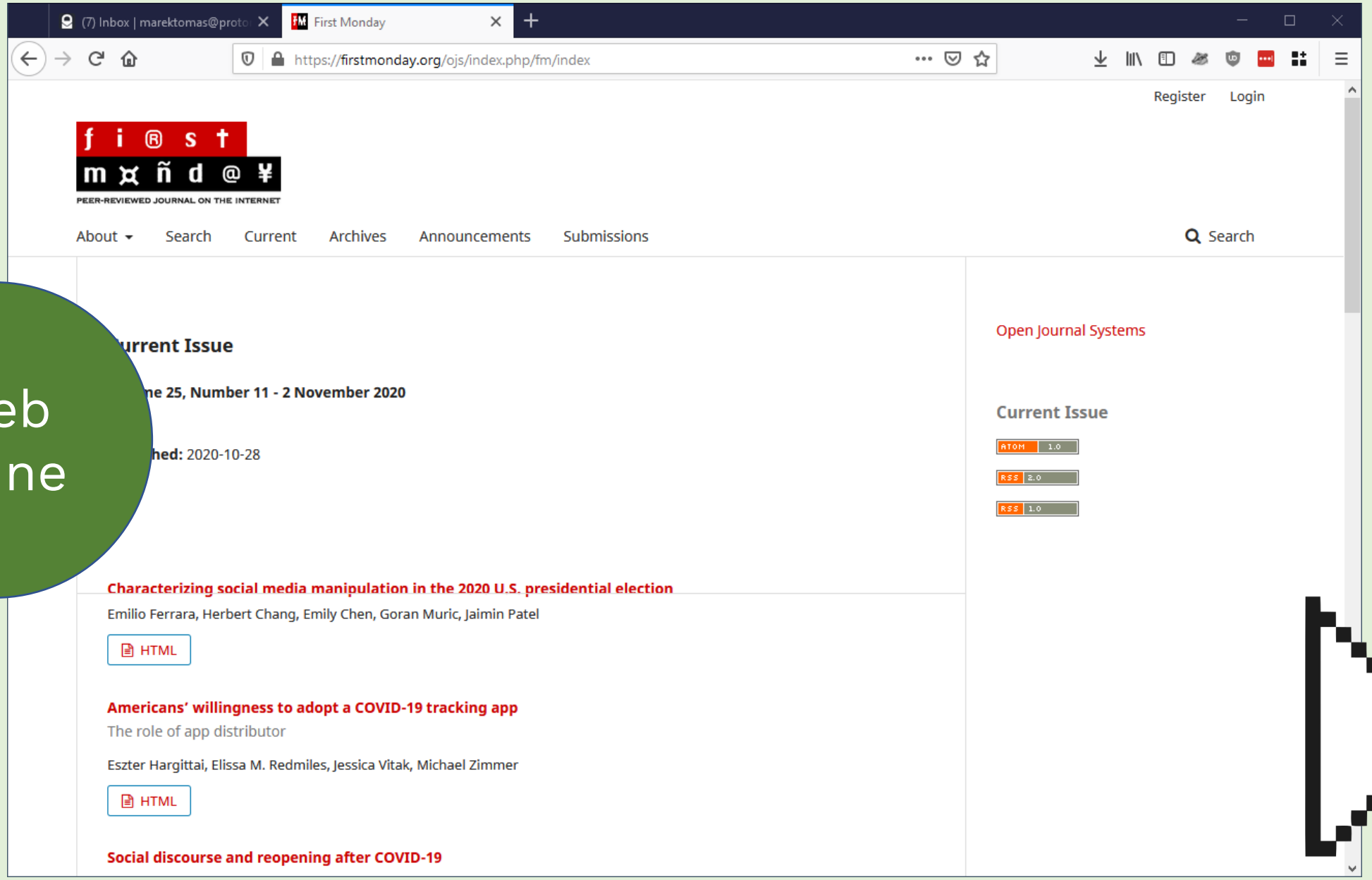
- **síťový HW**
- https://upc.michalspacek.cz/

- **fotoaparáty** - EXIF informace
- geolokace
- webkamera

čím více bezpečí a anonymity,
tím více nepohodlí

Co teď s tím vším?

Web týdne


(7) Inbox | marektomas@proto
First Monday
https://firstmonday.org/ojs/index.php/fm/index
Register
Login
first monday
PEER-REVIEWED JOURNAL ON THE INTERNET
About
Search
Current
Archives
Announcements
Submissions
Search
urrent Issue
ne 25, Number 11 - 2 November 2020
hed: 2020-10-28
Characterizing social media manipulation in the 2020 U.S. presidential election
Emilio Ferrara, Herbert Chang, Emily Chen, Goran Muric, Jaimin Patel
HTML
Americans' willingness to adopt a COVID-19 tracking app
The role of app distributor
Eszter Hargittai, Elissa M. Redmiles, Jessica Vitak, Michael Zimmer
HTML
Social discourse and reopening after COVID-19
Open Journal Systems
Current Issue
ATOM 1.0
RSS 2.0
RSS 1.0