Mobilní komunikace

Petr Matoušek
2017-06-05

Motivace

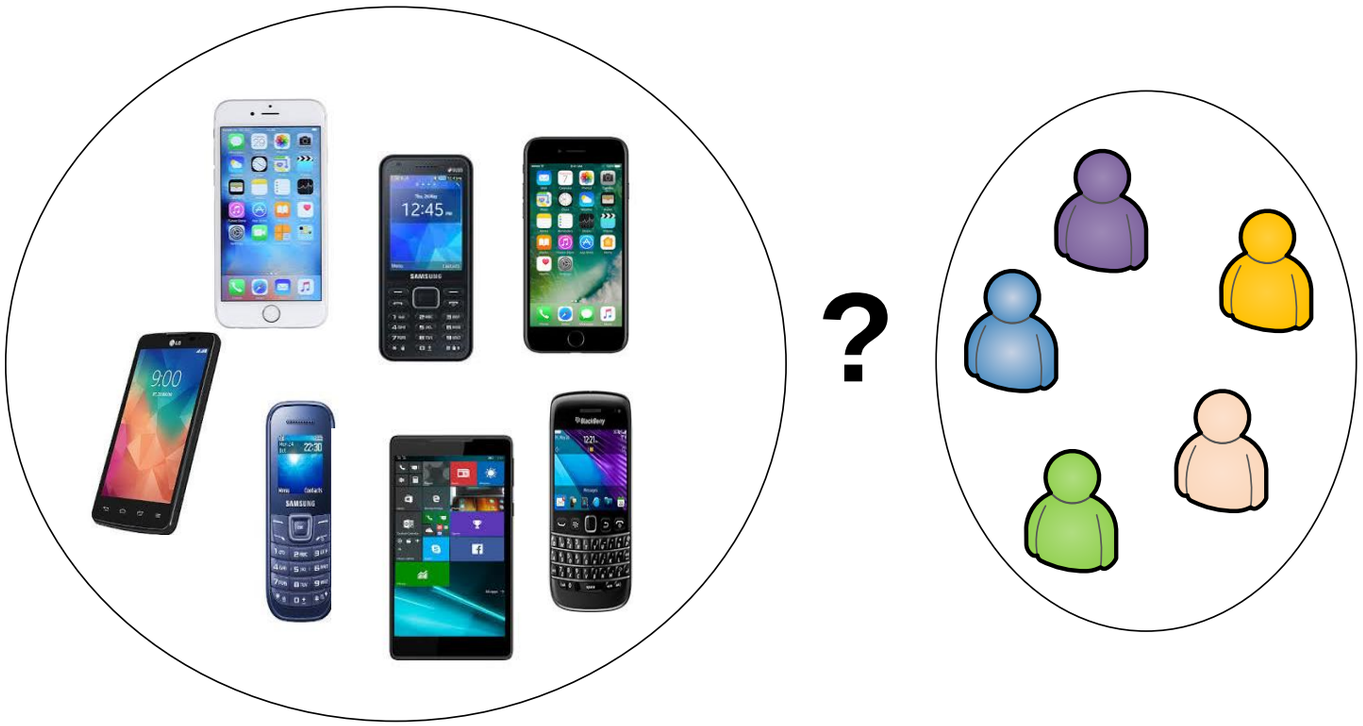
Mobilní telefony, chytré hodinky a další zařízení mohou být přímo nebo nepřímo součástí vyšetřování kybernetické kriminality.

Řešené problémy

1. *Můžeme prokázat, že dané mobilní zařízení patří konkrétnímu uživateli?*

   - Lze dokázat, že dané zařízení patří právě konkrétnímu člověku?

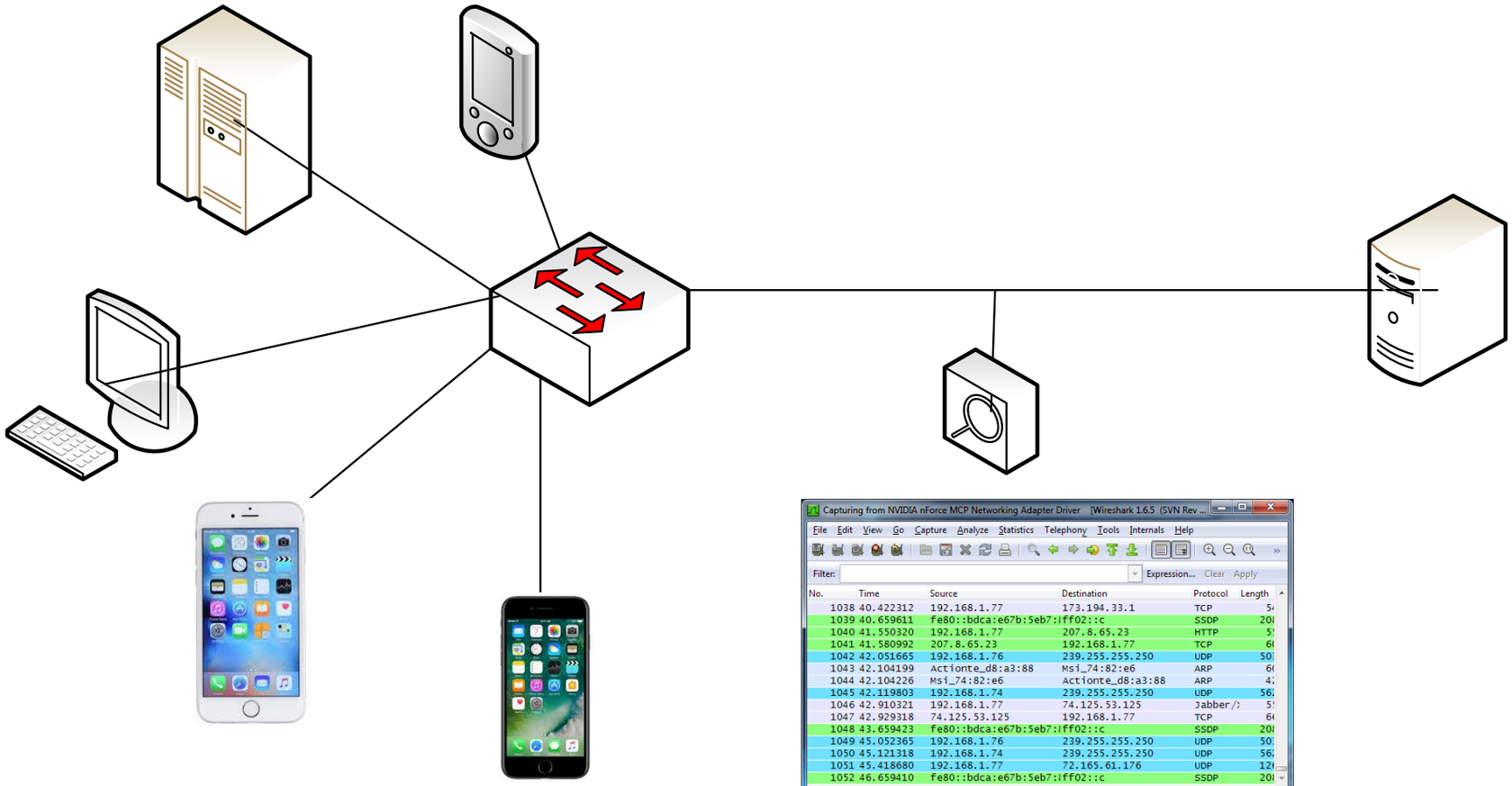
     -> tato otázka vede na *hledání otisku mobilního uživatele (mobile user fingerprinting)*



Řešené problémy

2. *Lze určit, že zachycený síťový provoz pochází z konkrétního zadrženého mobilního zařízení?*

   - Toto vede na kombinace síťové a mobilní forenzní analýzy.



1 Identifikace uživatele mobilního zařízení

1.1 Otisk mobilního zařízení

- Hypotéza: *Každý uživatel mobilního zařízení má vlastnosti, které vyjadřují jeho osobnost, zkušenosti, preference životní styl, apod.*
- Tyto vlastnosti je možné detekovat v různém nastavení mobilního telefonu, z metadat týkající se používání zařízení, používaných aplikací a podobně.

1 Identifikace uživatele mobilního zařízení

1.1 Otisk mobilního zařízení

- Hypotéza: *Každý uživatel mobilního zařízení má vlastnosti, které vyjadřují jeho osobnost, zkušenosti, preference životní styl, apod.*
- Tyto vlastnosti je možné detekovat v různém nastavení mobilního telefonu, z metadat týkající se používání zařízení, používaných aplikací a podobně.

-> Hledáme množinu atributů (features) či vlastností (personal traits) na základě data získaných z mobilního zařízení, tzv. otisk uživatele.

- Tento otisk uživatele je možné srovnávat s dalšími otisky a stanovit míru podobnosti či shody.
- Srovnání může prokázat či vyvrátit, zda dané zařízení patří té stejné osobě.

1 Identifikace uživatele mobilního zařízení

1.1 Otisk mobilního zařízení vs. otisk uživatele zařízení

Otisk mobilního zařízení: hodnotíme různé fyzické vlastnosti a nastavení mobilního zařízení. Cílem je detekovat konkrétní zařízení.

1 Identifikace uživatele mobilního zařízení

1.1 Otisk mobilního zařízení vs. otisk uživatele zařízení

Otisk mobilního zařízení: hodnotíme různé fyzické vlastnosti a nastavení mobilního zařízení. Cílem je detekovat konkrétní zařízení

Podobné otisku webového prohlížeče – používá se k identifikaci uživatele webu.

- Používají e-shopy.
- Typické vlastnosti: typ prohlížeče, verze, installované pluginy, dostupné fonty, rozlišení obrazovky, cookies, podporované typy MIME, časová zóna, apod.

See Eckersley, P.: How unique is your web browser? In: Proceedings of the 10th International Conference on Privacy Enhancing Technologies. PETS'10, Berlin, Heidelberg, Springer-Verlag (2010) 1 – 8

Viz např. https://amiunique.org/fp

1 Identifikace uživatele mobilního zařízení

1.1 Otisk zařízení: Příklad nastavení iOS

- *Booleovské hodnoty*
  - Closed captioning enabled, guided access enabled, in-app purchases allowed, inverted colors enabled, language different from a country,mono audio enabled, twitter enabled, voiceOver enabled, VoIP allowed, jailbreak, Internet connection type
- *Retězce*
  - Carrier name, current ISP, current public IP, device country, device language, device model, device name, iOS version, WiFi SSID, photo album titles, reminder list names, twitter account name
- *Seznamy*
  - Installed apps (icon cache), installed apps (URL schemes), installed keyboards, top 50 songs, calendar names, contacts

See Kurtz, A., Gascon, H., Becker, T., Rieck, K., Freiling, F.: Fingerprinting mobile devices using personalized configurations. Proceedings on Privacy Enhancing Technologies (2016) 4-19

1 Identifikace uživatele mobilního zařízení

1.1 Využití pro správu přístupů (Access Management)

Jaké vlastnosti lze použít? (test na 59 uživatelích)

Fingerprint Component	No of distinct values	Max. identical values
screen dimension + color dep	27	17
timezone	2	58
installed plugins	4	50
vendor	4	40
installed fonts	7	37
browsersLanguage	3	53
appMinorVersion	2	53
systemLanguage	3	53
cpuClass	2	53
userLanguage	3	53
userAgent	47	5
appName	1	59
appCodeName	1	59
appVersion	47	5
buildID	3	56
platform	7	42
oscpu	2	56
product	1	59
productSum	3	50
language	10	13

See Hupperich, T., Maiorca, D., Kuhrer, M., Holz, T., Giacinto, G.: On the robustness of mobile device fingerprinting: Can mobile users escape modern web-tracking mechanisms? In: Proceedings of the 31st Annual Computer Security Applications Conference. ACSAC 2015, New York, NY, USA, ACM (2015) 191-200

1 Identifikace uživatele mobilního zařízení

1.2 Otisk uživatele mobilního zařízení

Otisk uživatele mobilního zařízení: hledáme osobnostní charakteristiky pro jednoznačné určení vlastníka (uživatele) daného zařízení.

- Zaměřujeme se na uživatele spíše než na zařízení
- Lze použít k identifikace uživatele, který má více zařízení
- Do určité míry lze použít vlastnosti z otisku mobilního zařízení

1 Identifikace uživatele mobilního zařízení

1.2 Otisk uživatele mobilního zařízení

Otisk uživatele mobilního zařízení: hledáme osobnostní charakteristiky pro jednoznačné určení vlastníka (uživatele) daného zařízení.

- Zaměřujeme se na uživatele spíše než na zařízení
- Lze použít k identifikace uživatele, který má více zařízení
- Do určité míry lze použít vlastnosti z otisku mobilního zařízení

Charakteristiky: *osobní preference, nastavení, přizpůsobení lze najít na mobilním zařízení*.

E.g.: preferované aplikace (webový prohlížeč, e-mailový klient, komunikační programy), seznam kontaktů, frekvence volání, posílání zpráv SMS, uživatelské nastavení (jazyk, časové pásmo), množina nainstalových aplikací, seznam navštívených WiFi sítí

1 Identifikace uživatele mobilního zařízení

1.2 Identifikace uživatele podle nainstalovaných aplikací

- Seznam nainstalovaných aplikací může hodně říci o uživateli zařízení.
  - *“Řekni mi, jakou knihu čteš. ..” –> “Řekni mi, jaké aplikace používáš ...“*

1 Identifikace uživatele mobilního zařízení

1.2 Identifikace uživatele podle nainstalovaných aplikací

- Seznam nainstalovaných aplikací může hodně říci o uživateli zařízení.
  - *“Řekni mi, jakou knihu čteš. ..” –> “Řekni mi, jaké aplikace používáš ...“*

1) Kategorie aplikací Google Play Store

- Google Store rozděluje dostupné aplikace podle kategorií a podkategorií.
- Podle kategorie aplikace lze odhadnout stav uživatele (svobodný, ženatý, s dětmi), jeho zájmy, oblíbené aktivity, apod.
- Např. náboženství, rodinný stav, pohlaví, věk dětí, zájmy, jazykové dovednosti, navštívená místa, apod.

Seneviratne, S., Seneviratne, A., Mohapatra, P., Mahanti, A.: Predicting user traits from a snapshot of apps installed on a smartphone. SIGMOBILE Mob. Comput. Commun. Rev. 18 (2014) 1-8

1 Identifikace uživatele mobilního zařízení

1.2 Identifikace uživatele podle metadat

2) Stanovení osobnosti uživatele pomocí metadat z mobilního zařízení

- Velká pětka (Big five): otevřenost vůči zkušenostem, svědomitost, extravertnost, přívětivost, neuroticismus
- Četnost užívání kancelářských aplikací, Internetu, SMS zpráv, her.
- Počet unikátních spojení přes Bluetooth, doba přenosu, četnost spojení
- Počet příchozích a odchozích zpráv SMS, průměrná délka, medián slovní délky
- Počet příchozích, odchozích, zmeškaných hovorů, délka trvání, počet unikátních hovorů, počet zmeškaných či odmítnutých hovorů.

Chittaranjan, G., Blom, J., Gatica-Perez, D.: Who's who with big-five: Analyzing and classifying personality traits with smartphones. In: 2011 15th Annual International Symposium on Wearable Computers. (2011) 29-36.

Otisk uživatele mobilního zařízení: Shrnutí

Dva typy otisků:

1. Otisk zařízení
   - Slouží k určení konkrétního mobilního zařízení.
   - Otisk tvoří fyzické a technické parametry.
   - Lze použít omezeně k identifikaci uživatele vlastnícího více zařízení.

2. Otisk uživatele na zařízení
   - Zaměřuje se na osobnostní rysy, osobní preference a zvyklosti.
   - Zkoumaná data vypovídají o osobnosti uživatele a jsou nezávislá na typu zařízení
   - Může být použito k identifikaci uživatele vlastnícího více zařízení.

2 Identifikace síťového provozu

Lze určit, zda zachycený síťový provoz pochází z konkrétního mobilního zařízení?

- Having a captured network traffic we would like to relate it to a specific mobile hardware (source of data).

Výzkumné otázky

- *Lze rozlišit síťový provoz z mobilního zařízení od provozu z klasického počítače či notebooku?*
- *Jaké jsou typické charakteristiky takového provozu?*
- *Lze jednoznačně určit mobilní zdroj odchyceného síťového provozu?*

2 Identifikace síťového provozu

2.1 Jak identifikovat síťový provoz z mobilního zařízení?

- Provedli jsme několik testů

Pár pozorování z testů

1) Identifikace v síti LAN

- MAC adresa: OUI výrobce odhalí, že jde o mobilní zařízení
- Odposlechem komunikace DHCP získáme IP adresu mobilního zařízení
- DHCP posílá položku hostname (např. android-495c41ae3c289092)

2 Identifikace síťového provozu

2.1 Jak identifikovat síťový provoz z mobilního zařízení?

2) Identifikace v síti WAN

- *Řetězec User-agent v komunikaci HTTP*
  - Např. Dalvik/1.6.0 (Linux; U; Android 4.4.4; SM-G318H Build/KTU84P
  - Mozilla/5.0 (Linux; Android 4.4.4; SM-G318H Build/KTU84P), AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/33.0.0.0 Mobile Safari/537.36 (Mobile; afma-sdk-a-v6.4.1)

2 Identifikace síťového provozu

2.1 Jak identifikovat síťový provoz z mobilního zařízení?

2) Identifikace v síti WAN

- *Řetězec User-agent v komunikaci HTTP*
  - Např. Dalvik/1.6.0 (Linux; U; Android 4.4.4; SM-G318H Build/KTU84P
  - Mozilla/5.0 (Linux; Android 4.4.4; SM-G318H Build/KTU84P), AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/33.0.0.0 Mobile Safari/537.36 (Mobile; afma-sdk-a-v6.4.1)
- *Sledováním specifických dotazů DNS*
  - Překlad domén: mobile.twitter.com, cloudconfig.googleapis.com, android.clients.google.com, img.samsungapps.com, www.htc.com, config.inmobi.com, ads.mp.mydas.mobi, sdkm.w.inmobi.com, i.l.inmobicdn.net
- Tyto dotazy jsou posílány během aktualizace software na mobilním zařízení, při synchronizaci kalendáře, načítání webových stránek, apod.

2 Network Traffic Identification

2.1 Jak identifikovat síťový provoz z mobilního zařízení?

- Pokud jsme identifikovali mobilní provoz, jak určit zdroj tohoto provozu?

Jak hledat stopy síťové komunikace na mobilním zařízení?

- Statistika síťového připojení v logovacích souborech na mobilním zařízení
- Cache pamět webového provozu, stažené webové stránky, cookies
- Statistika poslaných a přijatých e-mailových zpráv – logování.
- Logování stažených mobilních aplikací.
- Seznam uživatelových účtů: e-mail, google, FB, a další.
- Seznam navštívených Wifi sítí

Děkuji za pozornost.