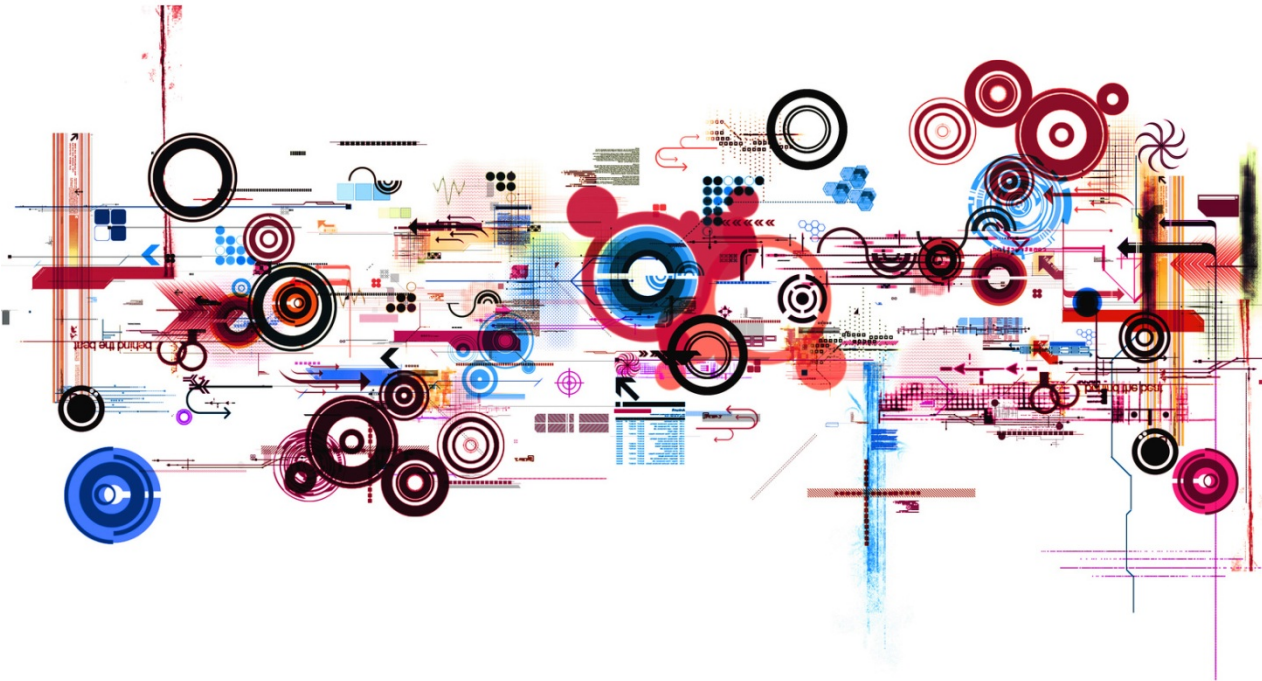


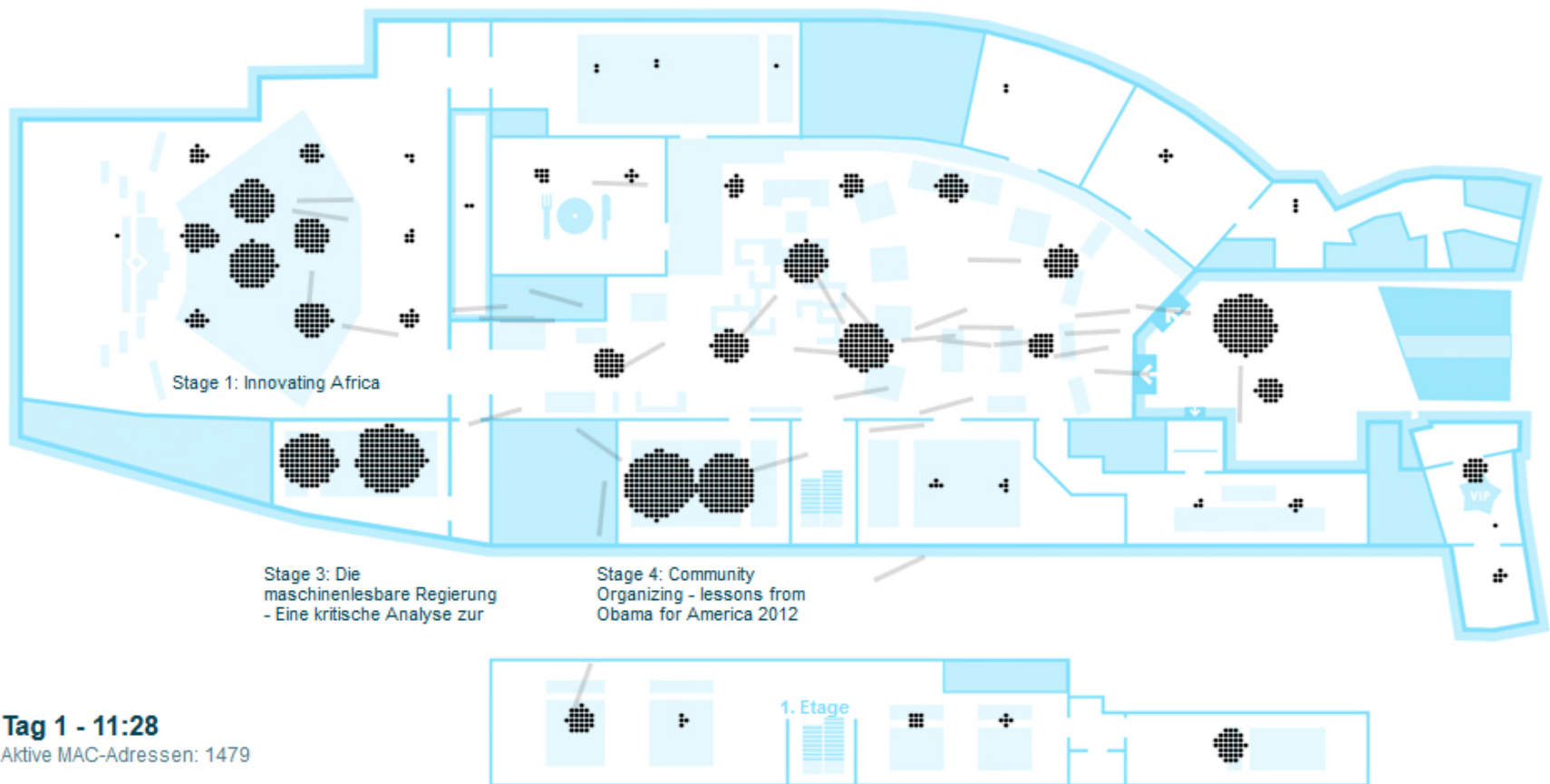
Tracking in freier Wildbahn

Von Leuchtfuern und Datenschleudern



Wimmelbild

Münchner Fachanwaltstag IT-Recht



Tag 1 - 11:28

Aktive MAC-Adressen: 1479

Quelle: re:log-Website. Realisiert von OpenDataCity.
Unterstützt durch picocell und newthinking. Anwendung steht unter CC-BY 3.0.

Funktionsweise



- Damit eine WLAN-Verbindung zustande kommen kann, müssen sich der Router (Access Point, AP) und das Endgerät „finden“.
- Der Router sendet in regelmäßigen Abständen sog. „Beacons“ (engl. „Blicklicht“, „Leuchtturm“) aus, die Informationen über den AP enthalten wie z.B. den Netzwerknamen (SSID).
- Ist das Endgerät im sog. „passiven Modus“, empfängt es diese Beacons und kann eine Verbindung herstellen.
Dazu muss das Endgerät jedoch regelmäßig den Empfangskanal wechseln, um den AP zu „sehen“.

Funktionsweise



- Viele Geräte mit WLAN-Schnittstelle arbeiten im sog. aktiven Modus und senden selbst in regelmäßigen Abständen sog. „Probe-Requests“, mit denen sie WLAN-Router suchen.
- Auch dies erfolgt auf allen WLAN-Kanälen, allerdings wartet das Gerät im aktiven Modus nur kurz (ca. 10 ms) auf eine Antwort und schaltet dann auf den nächsten Kanal. Dadurch ist der aktive Modus meist schneller im Verbindungsaufbau.
- Probe-Requests können gezielt an eine bestimmte SSID gerichtet sein oder sich als sog. Broadcast an alle APs in Reichweite richten.

Funktionsweise



- Für das WLAN-Tracking speichern APs (oder auch vermeintliche APs) die Probe-Requests von aktiv suchenden Geräten.
- Sind in einem Raum mehrere APs verteilt, lässt sich mit der an den einzelnen APs gemessenen Signalstärke sogar die Position des Geräts im Raum bestimmen.
- Bestandteil eines jeden Probe-Requests ist immer auch die **MAC-Adresse** des Endgerätes. Diese ist (zumindest bei Endgeräten in aller Regel) weltweit einmalig und ermöglicht die Verfolgung eines Gerätes im Raum.

Personenbezug der MAC-Adresse?



- Die MAC-Adresse ist eine 48 Bit lange Kennziffer. Sie besteht aus einer Herstellerkennung (24 Bit) und einem geräteindividuellen Teil (24 Bit).
- Art. 29-Gruppe:
„Die Kombination einer MAC-Adresse mit einem bekannten Access Point ist als personenbezogenes Datum zu behandeln.“
WP 185 S. 12 (Mai 2011)
- Ist das ein politisches Statement der Gruppe oder das Ergebnis einer rechtlichen Prüfung?

Personenbezug der MAC-Adresse?



- Art. 1 Abs. 2 Datenschutzrichtlinie 95/46/EG:
„Personenbezogene Daten sind alle Informationen über eine bestimmte oder bestimmbare natürliche Person.“
- Erwägungsgrund 26:
„Bei der Entscheidung, ob eine Person bestimmbar ist, sollten alle Mittel berücksichtigt werden, die vernünftigerweise entweder von dem Verantwortlichen für die Verarbeitung oder von einem Dritten eingesetzt werden könnten, um die betreffende Person zu bestimmen.“

Personenbezug der MAC-Adresse?



- § 3 Abs. 1 BDSG:
„Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener).“
- MAC-Adresse selbst ist ein geräte- bzw. bauteilbezogenes Datum. Im konkreten Fall identifiziert sie den Hersteller des WLAN-Moduls. Zwar lässt sich über die IEEE ermitteln, welchem Hersteller die MAC-Adresse zugeordnet ist, nicht aber wer das Gerät gekauft hat oder benutzt.

Exkurs: Bestimmbarkeit



- Absolute Theorie

Bestimmbarkeit ist gegeben, wenn irgendjemand (auch außerhalb der erhebenden/verarbeitenden Stelle) objektiv in der Lage ist, den Personenbezug herzustellen, selbst dann, wenn dies nur mit gesetzeswidrigen Mitteln möglich ist. (Weichert)

- Relative Theorie

Bestimmbarkeit ist nicht gegeben, wenn die erhebende/verarbeitende Stelle den Personenbezug selbst nur mit übermäßigen Aufwand herstellen kann. (Gola)

Personenbezug der MAC-Adresse?



- **Ohne weitere Zusatzinformationen ist die MAC-Adresse kein personenbezogenes Datum.**
- Die Art. 29-Gruppe schreibt selbst, dass die MAC-Adresse in dicht besiedelten Gebieten kein personenbezogenes Datum ist, meint aber, dass diese Feststellung nichts an der generellen Schlussfolgerung ändert, MAC-Adressen seien in Kombination mit einem konkreten Access Point als personenbezogene Daten zu behandeln sind.

Wann setzt der Personenbezug ein?



- Beispiel (1) nach Art 29-Gruppe:
Alleinstehendes Haus auf dem Land mit nur einem Bewohner
→ MAC-Adresse hat Personenbezug.
- Beispiel (2): re:publica-Snapshot
Weit überwiegend große Gruppen, vereinzelte Punkte, die aber ohne Zusatzwissen (z.B. Videoüberwachung) keiner Einzelperson zugeordnet werden können.
→ m.E. kein Personenbezug.

Wann setzt der Personenbezug ein?



- Beispiel (3): re:publica 4-Tage-Auswertung
Es ist möglich, die Bewegungen eines einzelnen Geräts über Tage zu verfolgen. Es bedarf weiterhin Zusatzwissens, um das Gerät einer bestimmten Person zuzuordnen, aber mit größerer Datenmenge wird das zusehends einfacher. Bei nicht aufbereiteten Daten m.E. wohl weiterhin kein Personenbezug.
- Durch die Veröffentlichung der animierten Daten im Internet kann hier jeder zugreifen und sich ggf. erinnern, mit wem er/sie am 1. Tag um 11:28 an der Essensausgabe stand ... dann liegt wohl der Personenbezug vor.

Exkurs: Was sagt das TKG dazu?



- Darf der AP (oder ein Fake-AP) den Probe-Request einfach so „abhören“?
- § 89 Abs. 1 Satz 1 TKG erlaubt das „Abhören“ von Nachrichten, die für die Allgemeinheit oder einen unbestimmten Personenkreis bestimmt sind.
- Probe-Requests richten sich an alle Empfänger im näheren Umfeld, so dass jedermann die Daten empfangen und abhören darf.

Vergleich zur Web-Analyse



- § 15 Abs. 3 TMG gestattet die Profilbildung auf Basis von
 - a) personenbezogenen Daten, sofern diese (in der Praxis: IP-Adresse)
 - b) für die Erbringung des Dienstes erforderlich sind
 - c) und die Profilbildung unter Pseudonym erfolgt.
Das Pseudonym darf dann nicht mit den Daten des Trägers zusammengeführt werden und
 - d) der Betroffene muss informiert werden und eine
 - e) Möglichkeit zum Widerspruch haben.

Vergleich zur Web-Analyse



- Beim WLAN-Tracking haben wir (m.E.)
 - a) keine personenbezogenen Daten
 - b) die Daten sind aber für die Erbringung „des Dienstes“ auch nicht erforderlich

Die Daten dürfen nicht mit personenbezogenen Daten des Nutzers zusammengeführt werden.

Bedarf es jetzt

- einer Information der Betroffenen?
- einer Möglichkeit zum Widerspruch?

Womit werben die Anbieter?



- Anonyme statistische Auswertung des Besucherverhaltens.
 - in einem Laden / Veranstaltungsort
 - im Einkaufszentrum / Fußgängerzone
 - der ganzen Stadt ...
- Erkennung wiederkehrender Besucher
- Wiedererkennung von Besuchern auch in anderen Shops / Städten / Ländern ...


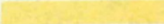



















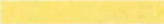












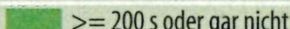

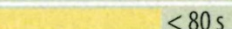


Lösungsansätze für die Praxis



- Keine zusätzlichen (ggf. identifizierenden) Daten über den Nutzer erheben; das gilt insbesondere für die Kombination z.B. mit Videoüberwachung.
- Ausfiltern von Mitarbeitern.
- Ausfiltern von Anwohnern.
- Unverzögliche Verschlüsselung der MAC-Adresse.
- technische Trennung von Händler und Tracking-Anbieter („Treuhänder“).
- Aggregation von Daten, Granularität reduzieren.
- Verzicht auf Dauertracking (wechselndes Salt).
- Information der Betroffenen, Opt-Out-Möglichkeit.

Nota bene: Was senden die Geräte so?



Trackbare WLAN-Aktivitäten der Smartphones und Tablets					
	Betriebssystem	verrät SSIDs	Scan-Häufigkeit (Standby)	Scan-Häufigkeit (aktiv)	Scan bei Lock / Unlock
Smartphones					
Apple iPhone 5c	iOS 8	–			✓ / ✓
Apple iPhone 5s	iOS 7.1.2	–			✓ / ✓
Google Nexus 5	Android 4.4.4	✓			✓ / ✓
HTC One M8	Android 4.4.2	–			– / –
Huawei Ascend P7	Android 4.4.2	–			– / ✓
LG G3	Android 4.4.2	–			– / ✓
Motorola Moto G	Android 4.4.2	–			– / ✓
Nokia Lumia 630	Windows Phone 8.1	✓ ²			✓ / ✓
Samsung Galaxy S5	Android 4.4.2	–			– / ✓
Sony Xperia SP	Android 4.3	–			– / ✓
Sony Xperia Z2	Android 4.4.2	✓ ¹			– / ✓
Tablets					
Amazon Kindle Fire HD	Fire OS 3.0 (Android)	✓ ¹			– / ✓
Apple iPad Air	iOS 7.1.2	–			✓ / ✓
Asus MeMo Pad HD 7	Android 4.2.2	–			– / ✓
Google Nexus 7 2013	Android L Preview	✓			✓ / –
Samsung Galaxy Note 10.1 2014	Android 4.3	–			– / ✓
Samsung Galaxy Tab 3 7.0	Android 4.1.2	–			– / ✓
¹ nur zuletzt benutzte SSID ² nur bei Lock					
 ≥ 200 s oder gar nicht  < 200 s  < 80 s  < 50 s  ≤ 20 s					

Mit freundlicher Genehmigung des Heise Zeitschriften-Verlag GmbH & Co. KG.
Entnommen aus c't 21/2014.

Wie schütze ich mich?



- Bewusstes Aktivieren und Deaktivieren des WLAN-Empfängers. Bei Android sind dazu teilweise diverse Untermenüs zu durchklicken.
- Die Android-App „Pry-Fi“ sorgt dafür, dass Probe-Requestes mit zufälligen (falschen) MAC-Adressen erfolgen.
- Apple hat für iOS 8 eine ähnliche Funktion angekündigt, die im c't-Test (21/2014) jedoch noch nicht funktionierte.
- Guerilla: Die App „Pry-Fi“ hat eine Funktion „Go to war!“, die Tracker mit falschen MAC-Adressen überschwemmt (DDoS für echte Router?).

iBeacons



- iBeacons sind Sendeeinheiten, die wie APs konstant ihre eigene Kennung aussenden, aber selbst keine Daten empfangen oder aufzeichnen.
- Sind die Standorte von iBeacons kartographiert, können Apps, die Zugang zu diesen Standortinformationen haben, den Standort des Gerätes durch Triangulation feststellen.
- Funktion ist gut geeignet für die sog. Indoor-Navigation, da GPS in Gebäuden häufig nicht verfügbar ist.
- Nutzung erfordert immer eine App, die die empfangenen iBeacon-Daten auswertet.

iBeacons



- Die App erhebt personenbezogene (Standort-) Daten des Nutzers.
- Wenn man die App als Telemediendienst einstuft würde wieder § 15 Abs. 3 TMG greifen – d.h. eine pseudonomisierte Auswertung wäre möglich, ein Opt-Out müsste aber angeboten werden.
- Über die Datenschutzerklärung in der App kann entsprechend informiert werden.
- In der App kann – entsprechend klare Information der Nutzer vorausgesetzt – auch eine Einwilligung zur weiteren Nutzung eingeholt werden.

Noch Fragen?

SKW
Schwarz
Rechtsanwälte

Nikolaus Bertermann

SKW Schwarz Rechtsanwälte

Neues Kranzler Eck

Kurfürstendamm 21

D-10719 Berlin

T +49 (0)30 889 26 50 45

F +49 (0)30 889 26 50 10

n.bertermann@skwschwarz.de