PROPRIVACY
TEILVORHABEN TECHNIK

SIT-Mitarbeiter: Tobias Hahn, Dr. Benjamin Lange

Fraunhofer
SIT

ARBEITSBEREICHE IN PRO PRIVACY

Kommunikationsinhalte

Daten im Smart Home

Verbindungsdaten

Positionsdaten

1. KOMMUNIKATIONSINHALTE ÜBERBLICK

Kommunikationsinhalte werden übermittelt durch

- Telefon (Festnetz, VoIP, Mobiltelefon)
- E-Mail
- SMS
- Messaging-Dienste
- Chat und Voice-Chat
- Soziale Netzwerke

Bewertung:

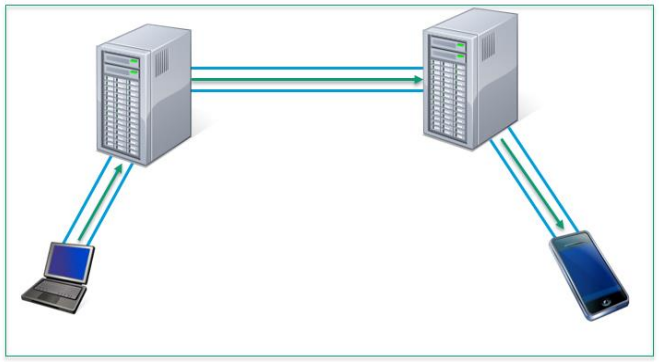
- Festnetzkommunikation häufig unverschlüsselt
- GSM-Verschlüsselung teilweise veraltet
- Messaging Dienst oft nicht Ende-zu-Ende verschlüsselt
- Ende-zu-Ende-Verschlüsselung zwar verfügbar, aber
  - mit Kosten verbunden
  - häufig nicht kompatibel
  - nicht nutzerfreundlich

1. KOMMUNIKATIONSINHALTE SCHWERPUNKT: E-MAIL-KOMMUNIKATION

Schutzmöglichkeiten:

1) Transportverschlüsselung

- E-Mail-Verkehr heute größtenteils TLS-verschlüsselt (2013: Nur 15% des deutschen E-Mail-Verkehrs TLS-verschlüsselt)
- Beispiel: E-Mail Made in Germany
- Transportverschlüsselung (TLS) weist häufig Schwächen auf
  - Kein Perfect Forward Secrecy
  - Veraltete Algorithmen (RC4 u.a.)
  - Fallback auf unsichere Algorithmen



Bewertung:

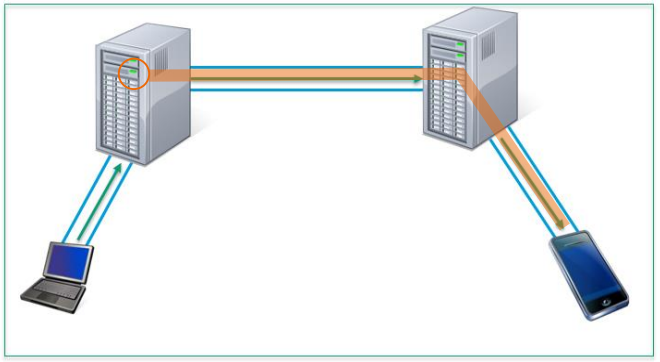
- Schutz vor Ausspähen auf den Teilstrecken
- Keine oder nicht durchgängige Transportverschlüsselung: E-Mails können im Klartext gelesen werden
- Durchgängige Transport-verschlüsselung: E-Mails bleiben für Provider lesbar

1. KOMMUNIKATIONSINHALTE SCHWERPUNKT: E-MAIL-KOMMUNIKATION

Schutzmöglichkeiten:

2) Nachrichtenverschlüsselung

- Einige E-Mail-Anbieter bieten E-Mail-Verschlüsselung an (z.B. Hushmail, Start-Mail, Tutanota, ProtonMail u.a.)
  - Schlüssel liegt Passwort-geschützt auf Servern der Anbieter; Nutzung von Webmailern (Javascript, Java-Applets)
  - Großer Nutzerkomfort
  - Lösungen häufig gar nicht oder schlecht mit Standardtechniken (PGP, S/MIME) kompatibel



Bewertung:

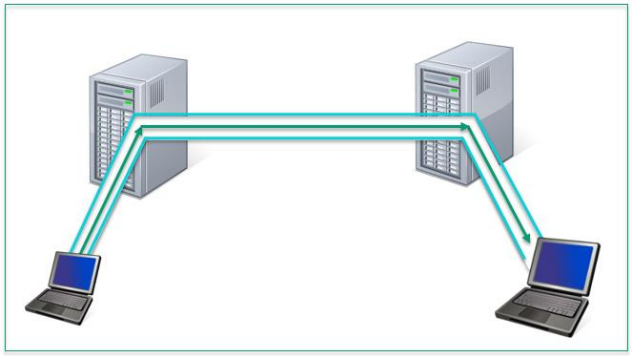
- Nachrichtenverschlüsselung kann vor Providern schützen
- Anbieter hat Möglichkeiten, in den Besitz des geheimen Schlüssels zu kommen

1. KOMMUNIKATIONSINHALTE SCHWERPUNKT: E-MAIL-KOMMUNIKATION

Schutzmöglichkeiten:

3) Ende-zu-Ende-Verschlüsselung

- Verschlüsselung unabhängig von E-Mail-Anbieter durch vertrauenswürdige Software (z.B. Mailpile, GPG4Win, Enigmail, Mailvelope u.a.)
  - Verfügbar als
    a) eigenständiger E-Mail-Client
    b) Add-on/Plugin in E-Mail-Clients oder Browsern
  - Schlüssel liegt Passwort-geschützt auf dem Endgerät des Nutzers
  - Kein großer Nutzerkomfort
  - Problematische Schlüsselverwaltung und Schlüsselverteilung



Bewertung:

- Schutz vor Ausspähen auf Teilstrecken
- Schutz vor Providern und unbefugten Dritten
- Fehlende Nutzerfreundlichkeit verhindert flächendeckenden Einsatz

1. KOMMUNIKATIONSINHALTE FAZIT

Bewertung und Verbreitung bestehender Schutzmechanismen

- Kommunikationsinhalte sind gar nicht, unsicher oder unzureichend geschützt
- Verfügbare Schutzmaßnahmen sind häufig nicht nutzerfreundlich genug
- Starke Segmentierung bestehender Schutzmechanismen (mangelnde Kompatibilität)

Verbesserungsmöglichkeiten zum Schutz der Privatsphäre

- Einfach zu bedienende Ende-zu-Ende-Verschlüsselung durch eigenständige und vertrauenswürdige Software (Installation, Schlüsselerzeugung, verschlüsselte Kommunikation)
- Einfache Schlüsselverwaltung (z.B. halbautomatisierte Schlüsselverteilung)
- Einfacher und einheitlicher Schlüsselaustausch (z.B. über DANE, DNSSEC)

2. SMART-HOME ÜBERBLICK

Smart Home umfasst die folgenden Technologien

- Gebäudeautomation (Alarmanlage, Beleuchtung, Rollläden, Heizung, etc.)
- Smart Metering
- Vernetzte Haushaltsgeräte
- Vernetzte Spielekonsolen
- Smart-TVs

Bewertung:

- Datensammlung in der Wohnung ist eine Bedrohung für die Privatsphäre
- Kaum Konfigurationsmöglichkeiten für Datenschutz
- Nur begrenzte Verwendung von Verschlüsselung
- Sicherheitstechnik weist häufig Mängel auf
- Häufig keine gute Sicherheitstechnologien verfügbar
- Ausspionieren möglich durch Dienstbetreiber, Gerätehersteller oder unbefugte Dritte

2. SMART HOME SCHWERPUNKT: SMART-TVS

Eigenschaften von Smart-TVs:

- Verbindung von klassischem Fernsehen und Internet (HbbTV-Inhalte über den „Red Button“)
- Smart-TV als Multimedia-Plattform (Fernsehen, Internetsurfen, Online-Banking, Shoppen, Apps, Zugriff auf eigene Musik, Filme, Bilder, etc.)
- Umfangreiche Sensoren (Kamera, Mikrophon, Stimm- und Gesichtserkennung, Bewegungs-, Temperatur- und Luftfeuchtigkeitssensoren)

Bewertung:

- Trotz Internetfähigkeit schlechterer Schutz als in klassischen Internetszenarien (z.B. Browser)
- Intransparente und defizitäre Einstellmöglichkeiten
- Einfache Trackingmöglichkeiten durch Cookies
- Datensammlung möglich durch
  - Gerätehersteller
  - Sender
  - Inhaltsanbieter (über Apps, Internetseiten)
  - Trackingprogramme von Dritten
  - Hacker in Reichweite des Netzwerks

2. SMART HOME
FAZIT

Bewertung und Verbreitung bestehender Schutzmechanismen

- Smart-Home-Geräte meist gar nicht oder unzureichend geschützt
- Intransparenz in der Datenübermittlung und in den Einstellmöglichkeiten
- Nutzer sind sich der Gefahren nur unzureichend bewusst

Verbesserungsmöglichkeiten zum Schutz der Privatsphäre

- Sensibilisierung für Gefahren
- Konsequente Umsetzung der bekannten Sicherheitstechniken im Umfeld von Smart Home (Verschlüsselung, Authentisierung, Konfigurierbarkeit, etc.)
- Privacy-Gateways zur Überwachung des ausgehenden Datenverkehrs

3. VERBINDUNGSDATEN ÜBERBLICK

Metadaten beinhalten Informationen über andere Daten:

- Empfänger, Sender (E-Mail, Chat)
- Telefonnummern (Telefon/SMS)
- IP-Adressen, Webseiten (Internetnutzung)

Analyse von sozialen Verbindungen und Aktivitäten der Nutzer durch

- Dienstbetreiber
- Unbefugte Dritte

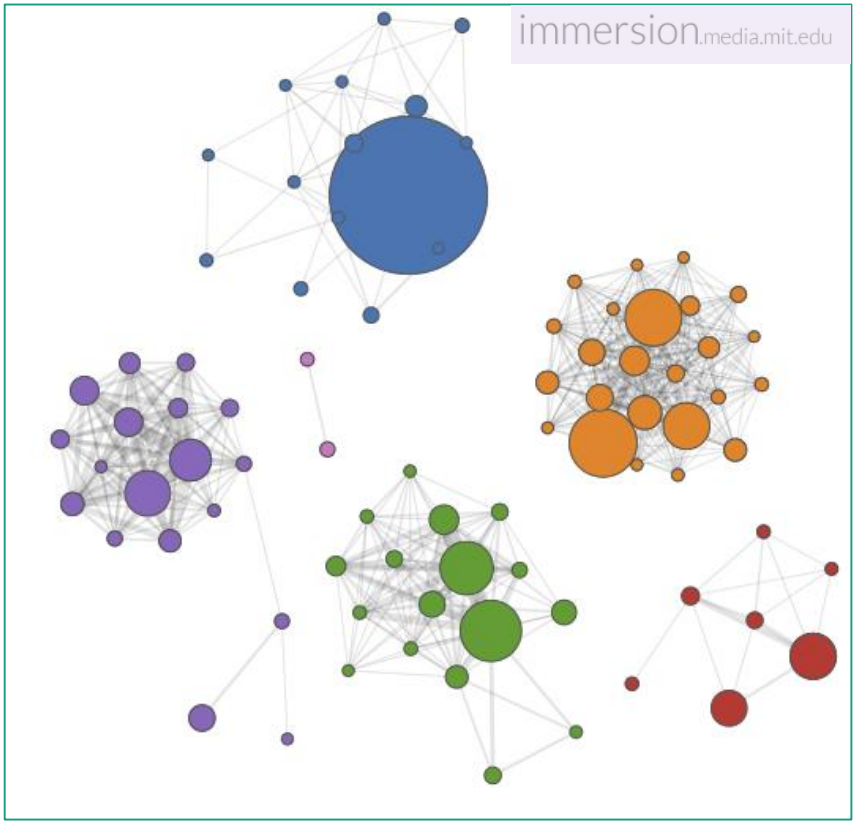
Metadaten sind sehr aussagekräftig

- Wer hat wann mit wem wie oft (worüber) kommuniziert?
- “Metadata tells you everything about somebody's life. If you have enough metadata, you don't really need content.” – Stewart Baker (NSA) 2013

3. VERBINDUNGSDATEN ÜBERBLICK

Analyse von Emails mit Immersion

- Entwickelt am MIT, frei verfügbar
- Erstellt aus Email-Headern Beziehungsgraphen
- Gute Visualisierung der möglichen Folgen der Überwachung der Verbindungsdaten



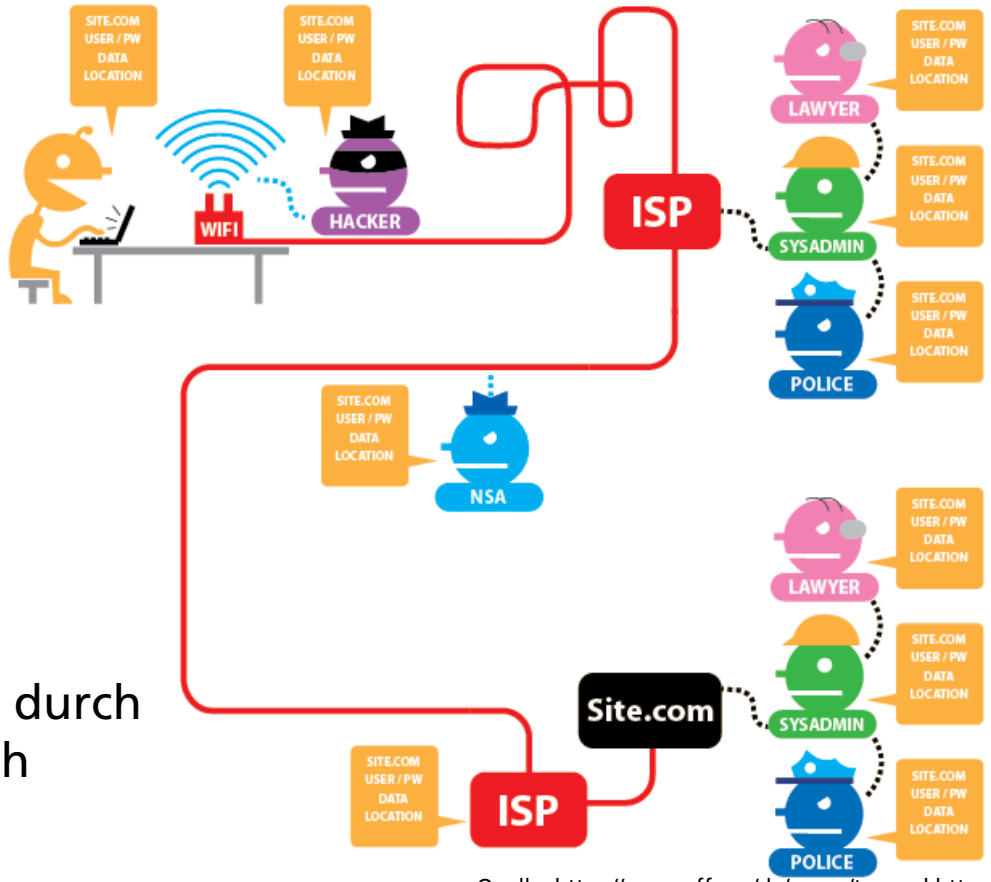
3. VERBINDUNGSDATEN – SCHWERPUNKT: INTERNET-KOMMUNIKATION

Nutzung eines Browsers zum Zugriff auf Webseiten

Anfallende Verbindungsdaten

- Adresse des Servers und der aufgerufenen Webseite
- Datum und Uhrzeit
- IP-Adresse, Cookies

Zugriff an verschiedenen Stellen durch unterschiedliche Akteure möglich



Quelle: https://www.eff.org/de/pages/tor-and-https

3. VERBINDUNGSDATEN – SCHWERPUNKT: INTERNET-KOMMUNIKATION

Verfügbare Schutzmechanismen

- HTTPS
- Privater Modus
- Proxy
- VPN

Bewertung

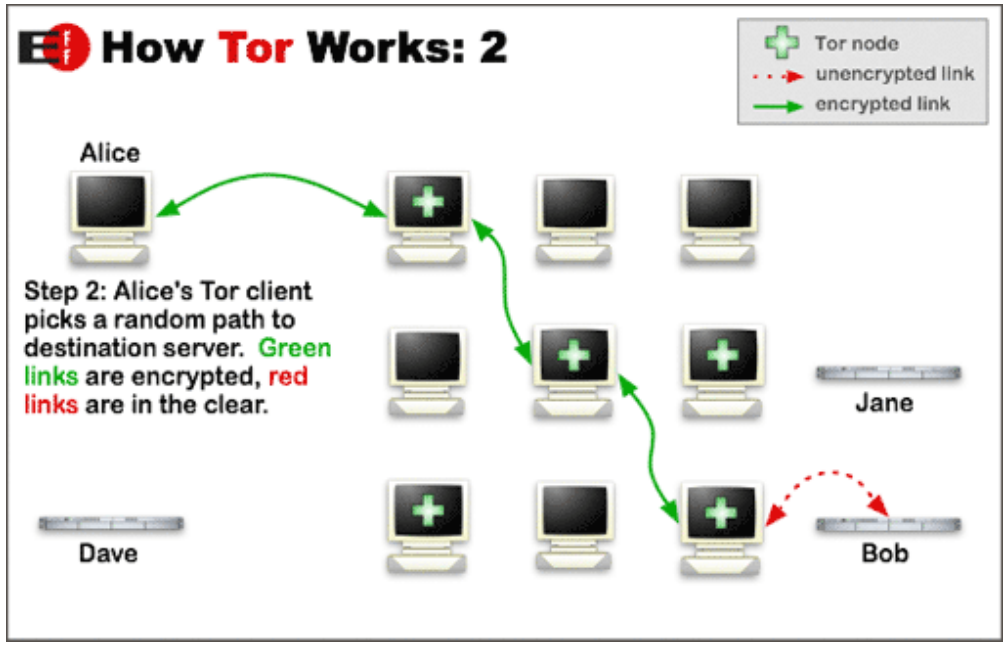
- HTTPS, Proxies, VPN oder privater Modus bieten keinen ausreichenden Schutz
- Identifizierung der Nutzer möglich, z.B. durch JavaScript
- Absolutes Vertrauen in VPN / Proxy-Betreiber erforderlich

3. VERBINDUNGSDATEN – SCHWERPUNKT: INTERNET-KOMMUNIKATION

Anonymisierungsdienste: Tor & JonDonym

- Weiterentwicklung des „Onion Routing“ (Syverson et.al., 1998)

- Mehrfache Verschlüsselung der zu übertragenden Daten
- Mehrere Knoten zwischen Sender und Empfänger
- Letzter Schritt evtl. im Klartext

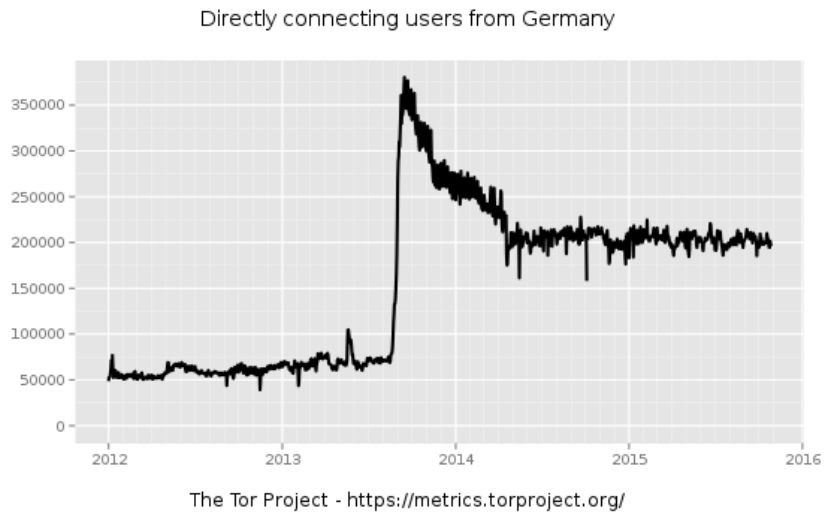


Quelle: https://www.torproject.org/about/overview

3. INTERNET-KOMMUNIKATION FAZIT

Bewertung und Verbreitung bestehender Schutzmechanismen

- Mit Tor bzw. JonDo existieren Tools, die dem Nutzer ein ausreichendes Schutzniveau bieten können
- Integration in Bundles / Spezial-Distributionen erhöhen den Schutz
- Geringe Nutzerzahlen; Tor: 200k Nutzer/Tag (0,036% der Internetnutzer), JonDo ~300 bzw. max. 2050 Nutzer



3. INTERNET-KOMMUNIKATION FAZIT

Bewertung und Verbreitung bestehender Schutzmechanismen

- Mit Tor bzw. JonDo existieren Tools, die dem Nutzer ein ausreichendes Schutzniveau bieten können
- Integration in Bundles / Spezial-Distributionen erhöhen den Schutz
- Geringe Nutzerzahlen; Tor: 200k Nutzer/Tag (0,036% der Internetnutzer), JonDo ~300 bzw. max. 2050 Nutzer

Konzepte für neue Technologien

- IP-Adressen-Anonymisierung mit angemessenem Nutzerkomfort und konfigurierbarem Schutzniveau
- Verdeutlichung der möglichen Folgen der Überwachung („Mini-NSA“)
- Steigerung der Benutzbarkeit durch Knoten bei Unis oder Netzbetreibern

4. POSITIONSDATEN ÜBERBLICK

Positionsbestimmung technisch möglich über

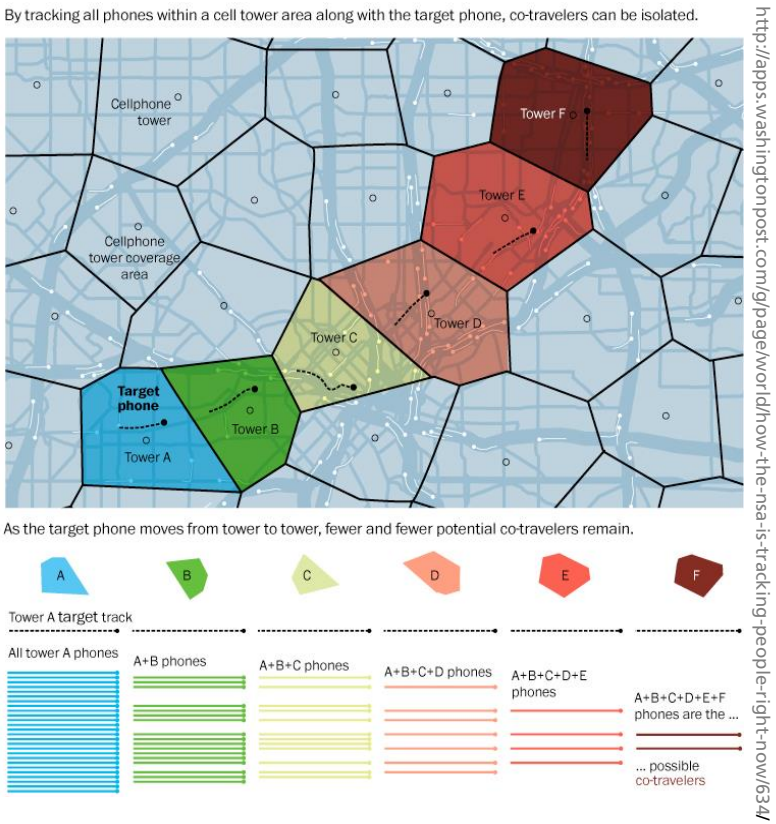
- WLANs in der Umgebung
- GPS-Empfänger
- Mobilfunknetz: Funkzellen, Triangulation, SS7
- IP-Adresse beim Internet-Zugriff
- Bluetooth (iBeacon)
- Stromverbrauch (experimentell)

Position wird bestimmt von

- Apps auf dem Smartphone
- Mobilfunkbetreibern
- Behörden
- Dritten (Hacker, Geheimdienste)

4. POSITIONSDATEN SCHWERPUNKT: SMARTPHONES

- Positionsbestimmung eines Smartphones mit vielen verschiedenen Techniken möglich
- Kombination verschiedener Techniken erhöht Genauigkeit
- Viele Nutzer (Juli 2015: 46 Mill.), die ihr Smartphone dauerhaft bei sich tragen.
- Positionsbestimmung auch ohne Möglichkeit zur Einflussnahme durch den Nutzer
- Detaillierte Profilbildung möglich, erlaubt Rückschlüsse auf Verhalten und Beziehungen



http://apps.washingtonpost.com/g/page/world/how-the-nsa-is-tracking-people-right-now/634/

4. POSITIONSDATEN SCHWERPUNKT: SMARTPHONES

Schutzmöglichkeiten

- Fake Location Apps verfügbar (GPS)
- Abschalten von WLAN, GPS, Bluetooth
- Positionsbestimmung per Mobilfunk teilweise erkennbar, nicht verhinderbar

Freigabe der Daten durch den Nutzer

- Foursquare; Facebook Places
  - Bewusstes Einchecken
- tinder: Ortsbasierte Dating-App
  - 2 Mil. Nutzer in Deutschland (Stand 01/2015)
  - Nutzer treten Rechte an Daten ab
  - Sicherheitslücken in der Vergangenheit

4. POSITIONSDATEN VON SMARTPHONES FAZIT

Bewertung und Verbreitung bestehender Schutzmechanismen

- Kaum Schutzmöglichkeiten vorhanden, meist Root/Jailbreak erforderlich
- Kein Schutz vor Positionsbestimmung durch Mobilfunknetz
- Freiwillige (aber evtl. uninformierte) Freigabe von Positionsdaten

Konzepte für neue Technologien

- Transparenz der Erfassung und Verarbeitung von Positionsdaten in Apps
- Sensibilisierung der Nutzer durch Veranschaulichung der Informationen die in den verarbeiteten Positionsdaten enthalten sind

ZUSAMMENFASSUNG

- Allgegenwärtige Überwachung durch verschiedene Player
- Nicht für alle Bereiche ausreichende Schutzmechanismen vorhanden (Smart Home und Positionsdaten)
- Vorhandene Techniken werden häufig nicht verwendet
  - Unkenntnis, Unklarheit der Bedrohung
  - Eingeschränkte Benutzbarkeit, technische Hürden bei der Einrichtung
- Notwendige Weiterentwicklungen
  - Verdeutlichung des Bedrohungspotentials, schaffen von Anreizen für die Nutzung der bestehenden Schutzmechanismen
  - Benutzerfreundliche Schutzmaßnahmen (alle)
  - Neuentwicklung von Schutzmaßnahmen im Bereich Positionsbestimmung und Smart Home

KONTAKTDATEN UND WEITERFÜHRENDE INFORMATIONEN

Dr. Benjamin Lange

- benjamin.lange@sit.fraunhofer.de

Tobias Hahn

- tobias.hahn@sit.fraunhofer.de

Abschlussbericht verfügbar unter

- http://sit4.me/proprivacy

Mail-Verteiler bei Fragen

- proprivacy@sit.fraunhofer.de