Munich Center for Internet Research (MCIR) Zwischenbericht Accountability

04.04.2017

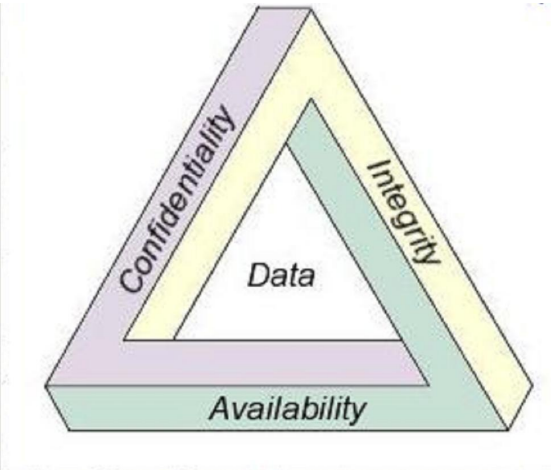
Ergebnisse des zweiten Sprints

- Erledigt:
  - Untersuchung der datenschutzrechtlichen Bedeutung und Zulässigkeit, insbesondere Betrachtung verschiedener Sensorarten und deren datenschutzrechtliche Relevanz
  - Zusammenspiel von Funktionssicherheit und Informationssicherheit in CPS
  - Accountability als Alternative zu üblichen Mechanismen (zB Verschlüsselung)
- Artefakte:
  - Flugfähige Drone mit Logginginfrastruktur
  - Besseres Verständnis der Probleme von ROSRV
  - Journalsubmission “Security for ROS” basierend auf dem Papier aus MCIR I
  - Konferenzsubmission zu Safety-Argumentationen von Drohnen

Produktsicherheit = Safety + Security?

- Grenze zwischen Safety und Security ist schwer zu ziehen.
- Safety: Schutz vor “natürlichen” Fehlern bzw. Schutz der Umwelt vor dem System
- Security: Schutz vor absichtlichen Angriffen bzw. Schutz des Systems vor der Umwelt
- Beispiel:
  - Ein Industrieroboter der mit Menschen arbeiten und, wenn Menschen in der Nähe sind, verlangsamt oder ganz stoppt.
  - Der Roboter bekommt von einem LIDAR folgende Werte gesandt:
    - 0, keine Menschen in der Nähe, arbeite mit voller Geschwindigkeit
    - 1, Menschen sind in der Kollaborationszone, arbeite mit geringer Geschwindigkeit
    - 2, Menschen sind zu nahe, Notstopp
  - Wenn ein Angreifer kann die Kommunikation manipulieren (was beispielsweise in ROS sehr leicht möglich ist), und immer den Wert 0 schicken
  - So wird ein Securityproblem, sehr schnell zu einem Safetyproblem

Accountability statt Security?



- CIA vs. AIC
  - Bei CPS ist oft Availability wichtiger als Integrity oder Confidentiality
  - n.b.: Datenschutz ist eng mit Confidentiality verknüpft
- Ist es möglich auf (teure) kryptographische Operationen zu verzichten?
  - z.B.: Verschlüsselung
- Beispiel:
  - Kann man durch entsprechende Logging-Maßnahmen sicherstellen, dass das Netzwerk frei von Angreifern ist, könnte man auf Verschlüsselung verzichten
  - So erreicht man nicht ein gleich hohes Schutzniveau, aber es kann “gut genug” sein.
  - Wie beschreibt man den Trade-off für solche “Adaptive Security”?
  - Kann man im “Ernstfall” komplexere Sicherheitsmaßnahmen “on demand” zuschalten?

Bildquelle
https://securitytoolkit.files.wordpress.com/2012/04/cia3.jpg

Datenquellen der *Runtime Verification*

- Unterscheidung zwischen Informationen die das CPS betreffen und Informationen die die Umwelt betreffen
- Unterscheidung zwischen personenbezogenen und sachbezogenen Daten

	personenbezogen	**sachbezogen**
Informationen die das CPS selbst betreffen	Ggf. Geographische Informationen über das CPS (GPS-Koordinaten und etwa Flughöhe), Fehlermeldungen	Betriebszeit, Systemtemperatur, Motordrehzahlen, Fehlermeldungen, Akkustand
Informationen die die Umwelt des CPS betreffen	Kommunikation mit der Bodensteuerungseinheit, **Umgebungserfassung mittels optisch-elektronischer Einrichtungen und sonstiger Sensorsysteme**	Windrichtung, Umgebungstemperatur

Datenschutzrechtliche Relevanz der Sensorik

- Im Rahmen von ROS: Range Finder (1D / 2D / 3D), Kameras, Audio/Speech Recognition, Bewegungserkennungssysteme
- Besondere Relevanz von Range Finder Systemen bei automatisierten CPS (insb. bei automatisierten Drohnen und automatisierten Fahrzeugen)

Bildquellen: http://ww1.prweb.com/prfiles/2014/11/14/12328795/XactMaps%20flys%20Velodyne.jpg, https://pics.computerbase.de/7/4/0/3/8/article-630x354.70f86e6b.jpg

Datenschutzrechtliche Relevanz der Sensorik

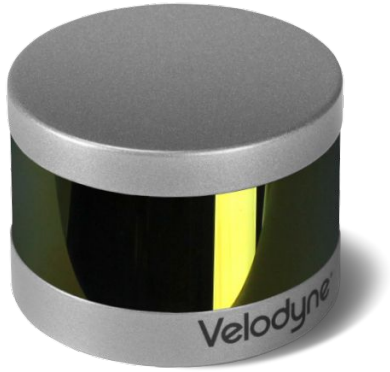
- Bei automatisierten Drohnen etwa:
  - Als Sense-and-Avoid System
  - Zur Erkennung von Überflugverboten
    (bspw. Menschenansammlungen (§ 21b Abs. 1 LuftVO-neu))
  - Zur Erkennung von Zielkoordinaten (bspw. bei Amazon Prime Air)

Bildquellen: http://media0.faz.net/ppmedia/1924260861/1.3865362/default/pegida-unterstuetzer-am-abend.jpg,
http://www.drohne-quadrocopter.de/wp-content/uploads/2015/12/Amazon-Drohne-Amazon-Prime-Air-Pakete-Waren_06_Landing-Area-Landezone.jpg

Datenschutzrechtliche Relevanz der Sensorik

- Erhebungsdimensionen bei Range Finder Systemen
  - 1D: Punktuelle Erfassung einer Tiefeninformation
  - 2D: Erfassung der Tiefeninformationen einer Achse
  - 3D: Erfassung der Tiefeninformationen auf allen Achsen

- Messmethoden bei Range Finder Systemen
  - Infrarot
  - Sonar (Schall)
  - **Stereo-Kameras**
  - **Lidar (Laser)**



Bildquellen: http://www.3dvision-blog.de/wp-content/uploads/2010/08/panasonic-limix-g-3d-lens-adapter-608x323.jpg, http://velodynelidar.com/images/products/vlp-16/puck.png

Datenschutzrechtliche Relevanz: Stereo-Kameras

- Datenschutzrechtliche Relevanz von Mono-Kameras unbestritten (bereits durch Aufnahme von Gesichtszügen unabhängig von Identifizierung oder Identifizierbarkeit)
- Bei Stereo-Kameras Steigerung der datenschutzrechtlichen Relevanz durch zusätzliche Tiefenebene

Bildquelle:
http://www.ingenieur.de/var/storage/images/media/ingenieur.de/bilder/der-volvo-v40-serienmaessig-fussgaenger-airbag-ausgestattet/4322215-1-ger-DE/Der-Volvo-V40-ist-serienmaessig-mit-einem-Fussgaenger-Airbag-ausgestattet_image_width_560.jpg

Auswege aus dem Datenschutz-Dilemma

- Verankerung der Grundsätze der Datensparsamkeit und der Datenvermeidung bereits bei der Technikgestaltung (“Privacy by Design”)
  - Bspw. unmittelbare Anonymisierung der Daten nach der Erhebung
  - Unmittelbare Löschung der Daten nach Wegfall der Erforderlichkeit
  - Verschlüsselte Datenspeicherung, wenn Daten längerfristig benötigt werden
- Strikte Einhaltung des Zweckbindungsgrundsatzes
- Rechtskonforme Technikgestaltung nach den Grundsätzen des BDSG und der DSGVO
- Technikadäquate Rechtsgestaltung?

Wer ist verantwortliche Stelle?

- Bspw. bei automatisierten Fahrzeug:
  - Hersteller des Fahrzeugs?
  - Halter?
  - Fahrer / Mieter / Leasingnehmer?
- Hersteller des CPS entscheidet im Rahmen der Entwicklung über Zweck und Mittel der Datenverarbeitung
  - Nur dieser hat ggf. Zugriff auf die Daten (bspw. per Remote-Zugriff)
  - Nur dieser kann Datensicherungsmaßnahmen nach § 9 BDSG ergreifen
  - Nur dieser weiß i.d.R. überhaupt, welche Daten in welcher Granularität erhoben, verarbeitet und genutzt werden

Technische Arbeit

- Erste Testflüge und Datenerfassungsflüge mit der Drohne
- Probleme beim Implementieren von bestehenden Runtime Verification ansätzen.
- Logging-funktionen sind implementiert
- Derzeit Arbeiten an der Auswertung der Logs
- Nächste Schritte:
  - Automatische Auswertung
  - Verträglichkeit mit dem Datenschutz
- Übernächste Schritte: Formalisierung von (relevanten) Gesetzen und passendes Reasoning

Ziele bis zum nächsten Sprint

- Höchste Priorität:
  - Formalisierung von rechtlichen Vorschriften (Beginn in diesem Sprint)
  - Datenschutzkonformität ausgewählter, spezifischer Anwendungsszenarien
  - Rechtsprozeduelle Fragen
    - Beweiskraft von Aussagen eines Accountability Mechnismus
    - Gerichtliche Verwertbarkeit der Ausgaben eines Accountability-Mechanismus
- Nebenläufige Tasks:
  - Case Study: Drohne
    - Recht und Technik auf die Drohne beziehen
    - “Kodifizierung des Rechts”: Im Simulator