Munich Center for Internet Research (MCIR) Zwischenbericht Accountability

30.05.2017

Ergebnisse des ersten Sprints

- Erledigt:
  - Datenschutzkonformität spezifischer Anwendungsszenarien
  - “Eigentum” oder sonst. Verfügungsbefugnis an den CPS-Daten?
- Nebenläufige Tasks:
  - Case Study: Drohne
    - Recht und Technik auf die Drohne beziehen
    - “Kodifizierung des Rechts”: Im Simulator
- Verschoben auf nächsten Sprint:
  - Rechtsprozeduelle Fragen (Dateneigentum vorgezogen!)
  - Formalisierung von rechtlichen Vorschriften

Datenschutzkonformität spez. Anwendungsszenarien

- Zur Erinnerung (Ergebnisse Sprint Review #7):
  - CPS erheben zahlreiche, auch personenbezogene, Daten
  - Dies gilt insb. bei Sterero-Kameras und 3D-Lidarsystemen (Tiefenebene)
  - Daher Verwendung nur i.R.d. Datenschutzrechts möglich
  - Datenschutzrechtlich Verantwortliche Stelle ist der CPS-Hersteller
  - Ggf. aber zusätzlich auch der Entwickler von Drittanbieter-Apps

- Datenschutzkonformität kann stets nur im Einzelfall für das konkrete Anwendungsszenario bewertet werden

- Daher Sprint Review #8:
  - Untersuchung zwei ausgewählter Anwendungsszenarien (“Menschenansammlung” und “Cloud-Tracing”)
  - Weiterhin: Bestehen eines “Dateneigentums” oder sonst. Verfügungsbefugnis an den CPS-Daten?

Anwendungsszenario: "Menschenansammlungen"

- § 21b Abs. 1 Nr. 2 LuftVO: *"Der Betrieb von unbemannten Luftfahrtsystemen und Flugmodellen ist verboten, […], über und in einem seitlichen Abstand von 100 Metern von Menschenansammlungen"*

- Erkennung von Menschenansammlungen?
  - Problematisch insbesondere: "Spontandemonstrationen" / zufällige Menschenansammlungen (keine Vorabinformation)
  - Erkennung nur durch optische Sensoren durch das CPS selbst möglich

- Datenschutzrechtliche Relevanz:
  - Permanente Bilddatenerfassung und -auswertung durch das CPS
  - Erfassung von Teilnehmern der Ansammlung selbst, aber auch außerhalb von Treffern, bspw. Passanten, Personen auf Privatgrundstücken, etc.
  - Identifizier**barkeit** wohl auch noch aus 100m Entfernung gegeben

- Einschlägiges Datenschutzrecht:
  - Derzeit BDSG bei nicht-öffentlichen Stellen
  - Ab Mai 2018: EU-DSGVO

Anwendungsszenario: "Menschenansammlungen"

- "Verbotsprinzip mit Erlaubnisvorbehalt"
  - Einwilligung? Ausgeschlossen, da zufällige, fremde Menschen
  - Gesetzlicher Erlaubnistatbestand?

- § 6b Abs. 1 BDSG: *"(1) Die **Beobachtung öffentlich zugänglicher Räume** mit **optisch-elektronischen Einrichtungen** (Videoüberwachung) ist nur zulässig, soweit sie [...] zur Wahrnehmung **berechtigter Interessen** für **konkret festgelegte Zwecke** erforderlich ist und keine Anhaltspunkte bestehen, dass **schutzwürdige Interessen der Betroffenen** überwiegen."*

- § 6b Abs. 1 BDSG weiter (seit 28.04.2017): "*Bei der Videoüberwachung von [...] öffentlich zugänglichen **großflächigen Anlagen**, wie insbesondere Sport-, **Versammlungs- und Vergnügungsstätten**, [...] gilt der **Schutz von Leben, Gesundheit oder Freiheit** von dort aufhältigen Personen als ein besonders wichtiges Interesse."*

Anwendungsszenario: "Menschenansammlungen"

- Problematisch aber § 6b Abs. 2 BDSG: *"Der Umstand der Beobachtung und die verantwortliche Stelle sind durch geeignete Maßnahmen erkennbar zu machen."*
  - *I.d.R. durch Hinweisschild unter (stationärer) Videokamera*

- Umsetzungsmöglichkeit bei UAS?
  - Aktives Aussenden einer eindeutigen ID?
  - Live-Tracking / Interaktive Flugkarten?

Bildquellen: http://www.rcheli-store.de/Multicopter/DJI-Phantom-Quadrokopter-RTF-Kit-Version-1-1-1.htm?shop=rcheli&a=article&ProdNr=RO-U4000&t=15578&c=15578&p=15578, http://www.lfd.niedersachsen.de/download/87309/Musterschild_Hinweis.pdf

Anwendungsszenario: “Menschenansammlungen”

- Außerhalb einer “Beobachtung” und außerhalb “öffentlich zugänglicher Räume”: Rückgriff auf § 28 Abs. 1 Nr. 2 BDSG

- Auch hier dann Interessensabwägung

- Diese kann insbesondere bei der Datenerfassung auf privatem Boden aber dann zugunsten des datenschutzrechtlich Betroffenen überwiegen!

Eigentum / Verfügungsbefugnis an den CPS-Daten

- I.R.d. automatisierten Fahrens derzeit äußerst umstritten; keine gefestigte Auffassung

- Frage nach einer güterrechtlichen Verfügungsbefugnis an Daten
  - "Wem gehören die von dem CPS generierten Daten"
  - Unabhängig von Eigentumsrechten am Datenträger
  - Unabhängig von Betroffenenrechten / inhaltlichen Rechten (bspw. Datenschutzrechten, Urheberrechten)

- Relevanz: Stünde das Dateneigentum / die Verfügungsbefugnis an den Daten nicht dem CPS-Hersteller zu, dürfte dieser die Daten nicht frei und ohne Einwilligung des Inhabers verwenden (etwa zur Produktverbesserung)

Existenz eines Daten"eigentums" i.e.S.

- § 903 Satz 1 BGB: *"Der Eigentümer **einer Sache** kann, soweit nicht das Gesetz oder Rechte Dritter entgegenstehen, mit der Sache nach Belieben verfahren und andere von jeder Einwirkung ausschließen."*

- § 90 BGB: *"Sachen im Sinne des Gesetzes sind **nur körperliche Gegenstände**."*
  - *Daten körperliche Gegenstände? Nein, da keine wahrnehmbare körperliche Abgrenzung*

- Ein "Dateneigentum" im wortwörtlichen Sinne existiert daher nicht

Existenz einer sonst. Verfügungsbefugnis an Daten

- § 823 Abs. 1 BGB: “Wer vorsätzlich oder fahrlässig das Leben, den Körper, die Gesundheit, die Freiheit, das Eigentum oder ein **sonstiges Recht** eines anderen widerrechtlich verletzt, ist dem anderen zum Ersatz des daraus entstehenden Schadens verpflichtet.”

- Daten als “sonstiges Recht”? Umstritten!
  - Vss.: Eigentumsähnlichkeit
  - Problem: Zuweisungs- und Ausschlussfunktion

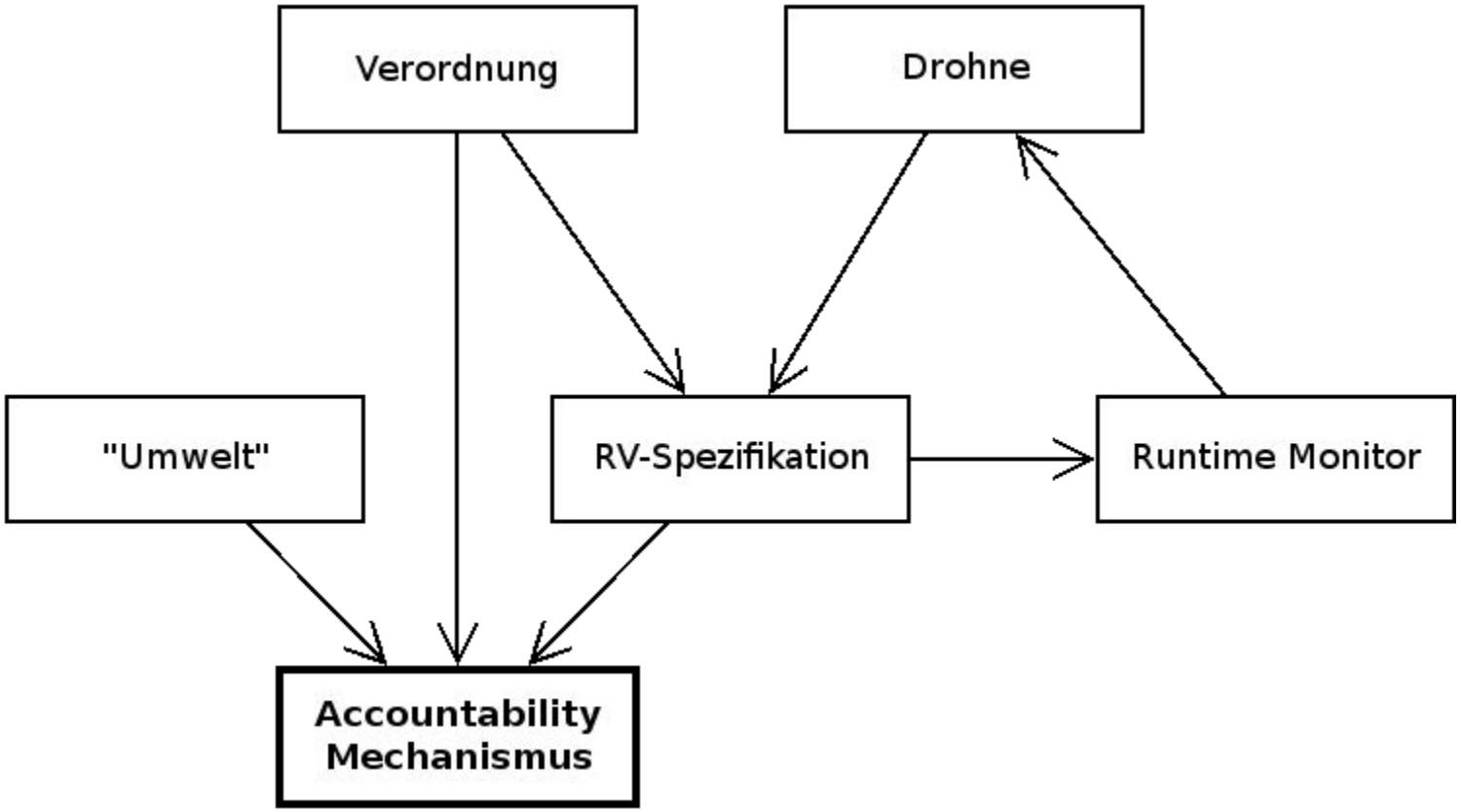
- Falls ja, wem gehören die CPS-Daten?
  - **Auffassung 1**: Dem Eigentümer des Datenträgers (aber problematisch bei etwa Clouddiensten oder beim Webhosting)
  - **Auffassung 2**: Nach den Betroffenenrechten (bspw. nach der datenschutzrechtlichen Betroffenheit) (aber: “Dateneigentum” soll etwa auch außerhalb personenbezogener Daten existieren)
  - **Auffassung 3**: Sog. “Skripturakt” (Begriff von 1988!): Inhaber ist der, der den Schaffungsprozess in Gang setzt. Dies soll laut einigen Stimmen im Schrifttum auch bei automatisierten Systemen stets der Nutzer sein, nicht der Hersteller (str.)

Existenz einer sonst. Verfügungsbefugnis an Daten

- Verfügungsbefugnis an Kopien?
  - Auch hier Abstellen auf “Skripturakt” (“wer hat die Kopie erschaffen”) (str.)
  - Verfügungsbefugter der Kopie (etwa auf eigenem Server) kann daher der CPS-Hersteller sein, auch wenn Verfügungsbefugter des Originals der CPS-Nutzer ist
  - Zur rechtmäßigen Anfertigung der Kopie aber ggf. vorherige Einwilligung des Verfügungsbefugten des Originals (CPS-Nutzer) notwendig
  - Daher ggf. umfassende Regelungen zwischen CPS-Hersteller und CPS-Nutzer in Nutzungsvereinbarungen notwendig (bspw. Zustimmung bei Erstinbetriebnahme)

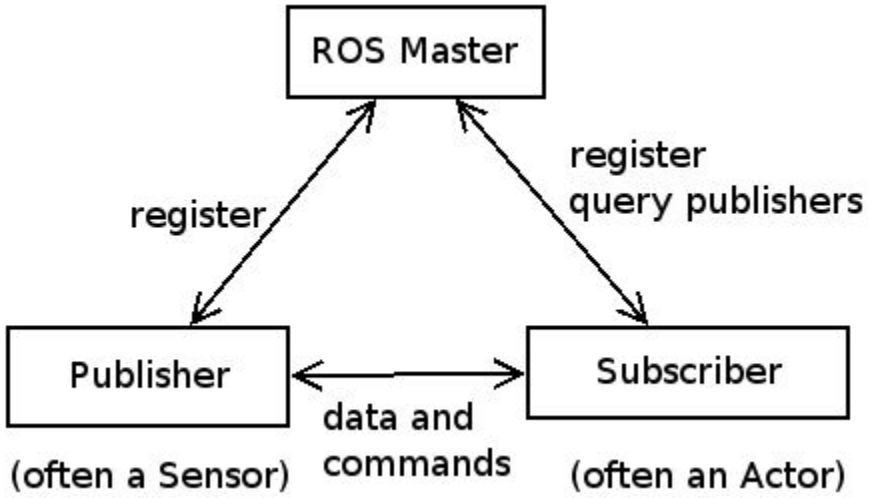
Zur Erinnerung: Runtime Verification

- Runtime Verification (RV) = Trace + System Spezifikation
- RV prüft ob sich das System gemäß der Spezifikation verhält



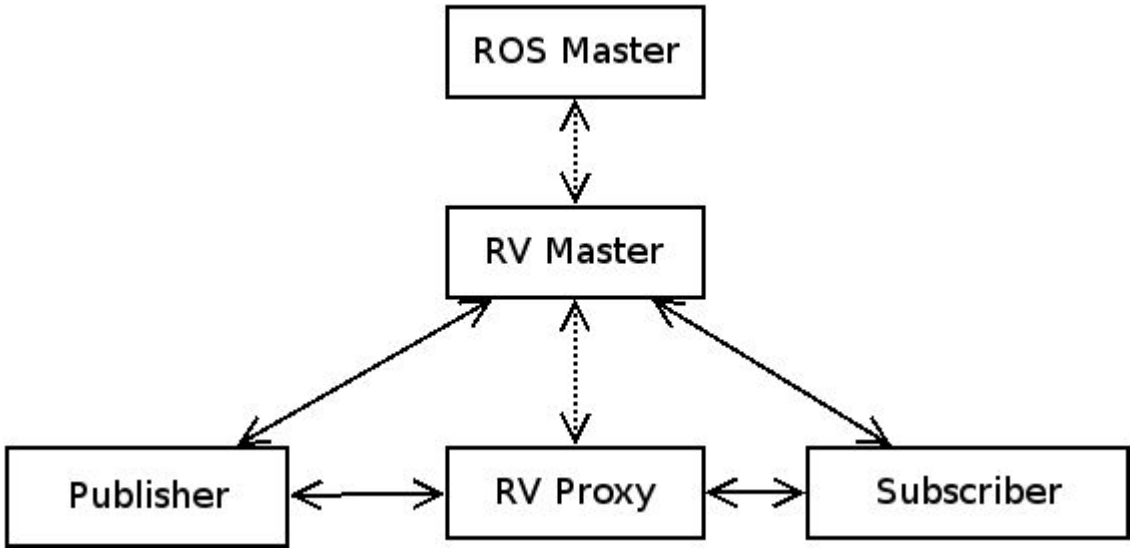
Technische Umsetzung von Runtime Verification

- Problem: Wo und wie greift man steurend ein?
- Kurze Einführung in die Architektur vom Robot Operating System:
  - Kommunikation via TCP oder UDP; meistens XMLRPC calls
  - Keine Sicherheits oder Safety Features



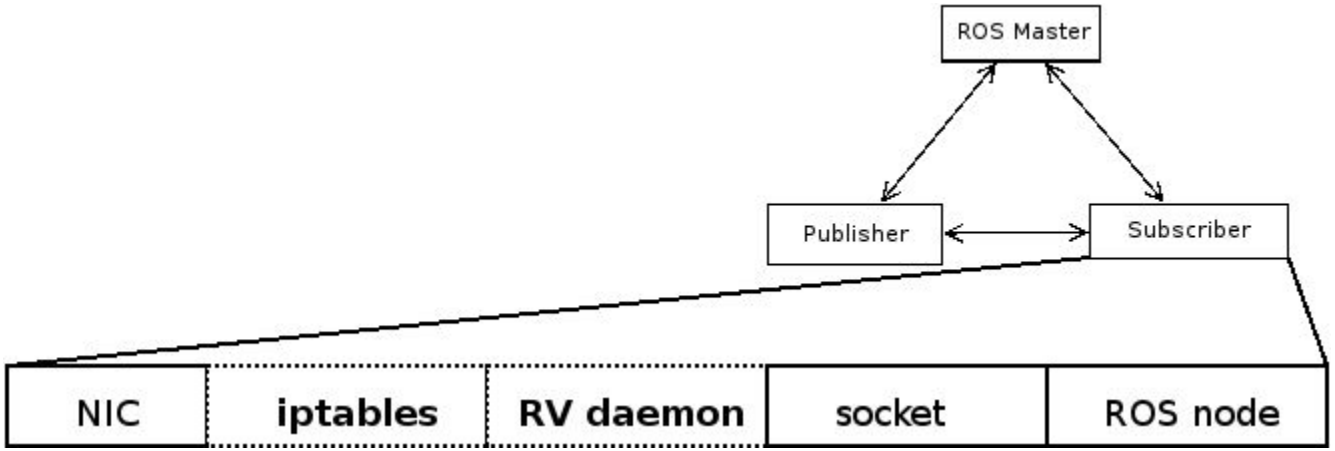
ROSRV

- Zentraler “Proxy” der Kommandos umschreiben kann
- Verlangt es die Netzwerktoplologie zu ändern
- Skaliert nicht



Unser Vorschlag

- Prüfung in der Netzwerkschicht der Aktoren vornehmen
- Machen aus dem “RV-Problem” ein Deep-Packet-Inspection Problem
- ROS Komponenten und Netzwerk müssen nicht geändert werden
- Vorteil: Daten sind zu diesem Zeitpunkt noch nicht “gespeichert”
- Offene Fragen:
  - Welche RV-checks können wir in diesem Setting ausführen?
    - RV checks sind “teuer” und müssen für jedes Packet gemacht werden
  - Wie gehen wir mit komplexeren/teureren Checks um?
  - Wie koordinieren wir die Checks über die Systemgrenzen hinweg?



Ziele bis zum nächsten Sprint

- Höchste Priorität:
  - Einsatz von Blockchains o. ä. Technologien um die Logs zu speichern

- “Übertrag” aus dem ersten Sprint:
  - Rechtsprozeduelle Fragen (Dateneigentum vorgezogen!)
  - Formalisierung von rechtlichen Vorschriften

- Nebenläufige Tasks:
  - Case Study: Drohne
    - Recht und Technik auf die Drohne beziehen
    - “Kodifizierung des Rechts”: Im Simulator