Heiko Mantels Baukasten für possibilistische Sicherheitsdefinitionen

Torsten Steinbrecher

Worum geht's?

- „possibilistische Sicherheitsdefinition“:
  aus der Beobachtung des Systems kann man mehrere mögliche tatsächliche Abläufe schließen $\Longrightarrow$ keine Schlussfolgerung möglich

- einfache Sicherheitsprädikate
  garantieren Nichtfolgerbarkeit bestimmter Verhalten auf hohem Sicherheitsniveau

- Sicherheitsprädikate
  sind Konjunktionen von einfachen Sicherheitsprädikaten.

- werden verschiedene poss. Sicherheitsdefinitionen zusammensetzen

„System“

- über einem Alphabet von Ereignissen, darunter Eingaben und Ausgaben
  (auf verschiedenen Sicherheitsniveaus)

- erlaubt eine Menge von Abläufen

- nichtdeterministisch
  aus einem Präfix eines Ablaufs folgt nicht unbedingt der Rest

- Ablaufmenge präfixabgeschlossen
  (klar: wenn $\alpha\beta$ ein möglicher Ablauf ist, dann auch α)

verschiedene Sicherheitsdefinitionen

- Vertraulichkeit:
  bestimmte Informationen (Ereignisse) auf hohem Niveau
  nicht auf niedrigem Niveau auslesbar oder folgerbar

- alles vertraulich $\Longrightarrow$ auch kein Informationsfluss von unten nach oben

- deshalb genau definieren:
  Was heißt, dass ein Beobachter auf niedrigem Niveau
  keine vertraulichen Informationen gewinnen kann?

- sinnvolle Sicherheitsdefinition systemabhängig

aus der Sicht eines Niedrigniveau-Beobachters

- vom Ablauf τ nur Projektion auf Niedrigniveau-Ereignisse $\tau|_L$ sichtbar
- Menge T möglicher Abläufe (inklusive Hochniveau-Ereignisse) bekannt
  (nix *security by obscurity* ;)
- Beobachter kann Niedrigniveauentsprechungsmenge konstruieren
  $LLES(T,\tau) = \{\tau' \in T \mid \tau'|_L = \tau|_L\}$
- Eigenschaften, die alle Abläufe in $LLES(T,\tau)$ teilen, folgerbar

Sicherheitsprädikate: Konjunktionen einfacher SPs

- ein einfaches Sicherheitsprädikat (Bauklotz) verlangt:
  für jeden Ablauf τ aus der Menge möglicher Abläufe T,
  für den eine gewisse Einschränkung $R_{ESP}(T,\tau)$ gilt,
  existiert ein (meist anderer) Ablauf τ' in $LLES(T,\tau)$,
  für den die Abschlussanforderung $Q_{ESP}(\tau,\tau')$ erfüllt ist

- $ESP(T) \equiv \forall\tau\in T: (R_{ESP}(T,\tau) \Longrightarrow \exists\tau'\in LLES(T,\tau): Q_{ESP}(\tau,\tau'))$

- $SP(T) \equiv ESP_1(T) \wedge ESP_2(T) \wedge \ldots$

zwei Sorten einfacher Sicherheitsprädikate

- vertraulich ist, dass ein Ereignis auf hohem Niveau stattfindet
  $\Longrightarrow$ Beobachtung ändert sich nicht, wenn es doch nicht stattfindet
  $\Longrightarrow$ Ablauf ohne dieses Ereignis in LLES(T,τ) enthalten

- vertraulich ist, dass ein Ereignis auf hohem Niveau nicht stattfindet
  $\Longrightarrow$ Beobachtung ändert sich nicht, wenn es doch stattfindet
  $\Longrightarrow$ Ablauf mit diesem Ereignis in LLES(T,τ) enthalten

erste Sorte: Hochniveauereignisse können wegfallen

- Entfernung von Ereignissen (*removal of events,* RE):

  $R_{RE}(T,\tau) \equiv \top$

  $Q_{RE}(\tau,\tau') \equiv \tau'|_H = \varepsilon$

  also insgesamt:

  $RE(T) \equiv \forall\tau\in T: (R_{RE}(T,\tau) \Longrightarrow \exists\tau'\in LLES(T,\tau): Q_{RE}(\tau,\tau'))$

  $RE(T) \equiv \forall\tau\in T\exists\tau'\in LLES(T,\tau): \tau'|_H = \varepsilon$

  kurz (inkorrekt, aber lesbar): $RE(T) \equiv \tau'|_H = \varepsilon$

- Entfernung von Eingaben (*removal of inputs,* RI):

  $R_{RI}(T,\tau) \equiv \top$

  $Q_{RI}(\tau,\tau') \equiv \tau'|_{HI} = \varepsilon$

  also insgesamt kurz: $RI(T) \equiv \tau'|_{HI} = \varepsilon$

erste Sorte: Hochniveauereignisse können wegfallen

- Entfernung von Ereignissen (*removal of events,* RE):

  $\mathrm{RE}(T) \equiv \tau'|_H = \varepsilon$

- Entfernung von Eingaben (*removal of inputs,* RI):

  $\mathrm{RI}(T) \equiv \tau'|_{HI} = \varepsilon$

- strenge Entfernung von Eingaben (*strict removal of inputs,* SRI):

  $R_{SRI}(T,\tau) \equiv \top$

  $Q_{SRI}(\tau,\tau') \equiv \tau'|_{HI} = \varepsilon \wedge \tau'|_{E\setminus HI} = \tau|_{E\setminus HI}$

  also insgesamt kurz: $\mathrm{SRI}(T) \equiv \tau'|_{HI} = \varepsilon \wedge \tau'|_{E\setminus HI} = \tau|_{E\setminus HI}$

erste Sorte: Hochniveauereignisse können wegfallen

- inkrementelle Löschung von Ereignissen (*deletion of events,* DE):

  $R_{DE}(T,\tau,\alpha,\beta,e) \equiv e \in H \wedge \tau = \beta e \alpha \wedge \alpha|_H = \varepsilon$

  $Q_{DE}(\tau,\tau',\alpha,\beta,e) \equiv \tau' = \beta\alpha$

  also insgesamt:

  $DE(T) \equiv$

  $\forall T \subseteq E^* \forall \tau \in T \forall \alpha,\beta \in E^* \forall e \in E:$

  $(R_{DE}(T,\tau,\alpha,\beta,e) \Longrightarrow \exists \tau' \in LLES(T,\tau): Q_{DE}(\tau,\tau',\alpha,\beta,e))$

  $DE(T) \equiv$

  $\forall T \subseteq E^* \forall \tau \in T \forall \alpha,\beta \in E^* \forall e \in E:$

  $((e \in H \wedge \tau = \beta e \alpha \wedge \alpha|_H = \varepsilon) \Longrightarrow \exists \tau' \in LLES(T,\tau): \tau' = \beta\alpha)$

  kurz (inkorrekt, aber lesbar): $DE(T) \equiv (e \in H \wedge \tau = \beta e \alpha \wedge \alpha|_H = \varepsilon) \Longrightarrow \tau' = \beta\alpha$

erste Sorte: Hochniveauereignisse können wegfallen

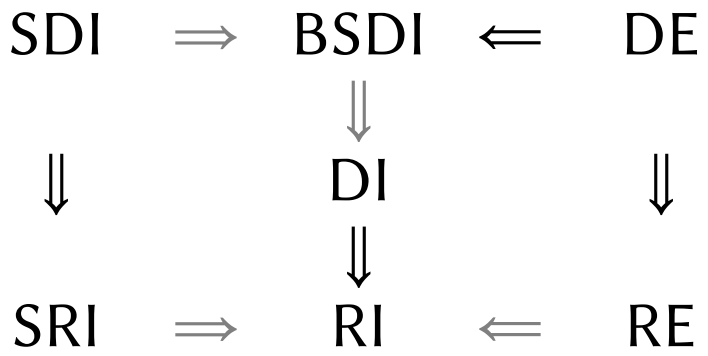
- inkrementelle Löschung von Ereignissen (*deletion of events*, DE):
  $\mathrm{DE(T)} \equiv (e \in H \wedge \tau = \beta e \alpha \wedge \alpha|_H = \varepsilon) \Longrightarrow \tau' = \beta\alpha$

- inkrementelle Löschung von Eingaben (*deletion of inputs*, DI):
  $\mathrm{DI(T)} \equiv (e \in H_I \wedge \tau = \beta e \alpha \wedge \alpha|_{H_I} = \varepsilon) \Longrightarrow (\tau' = \beta'\alpha' \wedge \beta'|_{H_I} = \beta|_{H_I} \wedge \alpha'|_{H_I} = \varepsilon)$

- strenge inkrementelle Löschung von Eingaben von hinten
  (*backwards strict deletion of inputs*, BSDI):
  $\mathrm{BSDI(T)} \equiv (e \in H_I \wedge \tau = \beta e \alpha \wedge \alpha|_{H_I} = \varepsilon) \Longrightarrow (\tau' = \beta\alpha' \wedge \alpha'|_{H_I} = \varepsilon)$

- strenge inkrementelle Löschung von Eingaben
  (*strict deletion of inputs*, SDI):
  $\mathrm{SDI(T)} \equiv (e \in H_I \wedge \tau = \beta e \alpha \wedge \alpha|_{H_I} = \varepsilon) \Longrightarrow \tau' = \beta\alpha$

erste Sorte: Hochniveauereignisse können wegfallen



- SDI(T) $\Longrightarrow$ SRI(T) sowie DI(T) $\Longrightarrow$ RI(T):
  wenn zu jedem τ ein τ' ohne die letzte Hochniveau-Eingabe existiert,
  dann existiert auch ein τ'' ohne Hochniveau-Eingaben

- DE(T) $\Longrightarrow$ RE(T):
  ersetze „Hochniveau-Eingabe“ durch „Ereignis auf hohem Niveau“

- DE(T) $\Longrightarrow$ BSDI(T):
  wenn zu jedem τ ein τ' ohne das letzte Hochniveau-Ereignis existiert,
  dann existiert auch ein τ'' ohne die letzte Hochniveau-Eingabe

zweite Sorte: Hochniveauereignisse können dazukommen

- Einfügung von Ereignissen (*insertion of events*, IE):
  $\mathrm{IE}(T) \equiv (e \in H \wedge \tau = \beta\alpha \wedge \alpha|_H = \varepsilon) \Longrightarrow \tau' = \beta e \alpha$

- Einfügung von Eingaben (*insertion of inputs*, II):
  $\mathrm{II}(T) \equiv (e \in H_I \wedge \tau = \beta\alpha \wedge \alpha|_{H_I} = \varepsilon) \Longrightarrow (\tau' = \beta' e \alpha' \wedge \beta'|_{H_I} = \beta|_{H_I} \wedge \alpha'|_{H_I} = \varepsilon)$

- strenge Einfügung von Eingaben von hinten
  (*backwards strict insertion of inputs*, BSII):
  $\mathrm{BSII}(T) \equiv (e \in H_I \wedge \tau = \beta\alpha \wedge \alpha|_{H_I} = \varepsilon) \Longrightarrow (\tau' = \beta e \alpha' \wedge \alpha'|_{H_I} = \varepsilon)$

- strenge Einfügung von Eingaben
  (*strict insertion of inputs*, SII):
  $\mathrm{SII}(T) \equiv (e \in H_I \wedge \tau = \beta\alpha \wedge \alpha|_{H_I} = \varepsilon) \Longrightarrow \tau' = \beta e \alpha$

zweite Sorte: Hochniveauereignisse können dazukommen

- problematisch beim Einfügen: alles kann eingefügt werden
  (nicht unbedingt sinnvoll)

- deshalb besser:
  nur solche Ereignisse dürfen eingefügt werden,
  die an dieser Stelle auf hohem Sicherheitsniveau zulässig sind

- auf hohem Niveau zulässiges Ereignis (*high-level admissible event,* HAE):
  $HAE(T,\beta,e) \equiv \exists \gamma \in E^*: (\gamma e \in T \wedge \gamma|_H = \beta|_H)$

- auf hohem Niveau zulässige Eingabe (*high-level admissible input,* HAI):
  $HAI(T,\beta,e) \equiv \exists \gamma \in E^*: (\gamma e \in T \wedge \gamma|_{HI} = \beta|_{HI})$

zweite Sorte: Hochniveauereignisse können dazukommen

- Einfügung auf hohem Niveau zulässiger Ereignisse
  (*insertion of high-level admissible events*, IHAE):
  $IHAE(T) \equiv (R_{IE} \wedge HAE(T,\beta,e)) \Longrightarrow Q_{IE}$
  $IHAE(T) \equiv (e \in H \wedge \tau = \beta\alpha \wedge \alpha|_H = \varepsilon \wedge \exists \gamma \in E^*: (\gamma e \in T \wedge \gamma|_H = \beta|_H)) \Longrightarrow \tau' = \beta e \alpha$

- Einfügung auf hohem Niveau zulässiger Eingaben
  (*insertion of high-level admissible inputs*, IHAI):
  $IHAI(T) \equiv (R_{II} \wedge HAI(T,\beta,e)) \Longrightarrow Q_{II}$

- BSIHAI und SIHAI entsprechend

zweite Sorte: Hochniveauereignisse können dazukommen

- problematisch bei Zulässigkeit auf hohem Niveau:
  γ darf sich auf niedrigem Sicherheitsniveau von β unterscheiden
  (nicht unbedingt sinnvoll)

- deshalb besser:
  nur solche Ereignisse dürfen eingefügt werden,
  die an dieser Stelle allgemein zulässig sind

- zulässiges Ereignis (*admissible event*, A):
  $A(T,\beta,e) \equiv \beta e \in T$

- Einfügung zulässiger Ereignisse (*insertion of admissible events*, IAE):
  $IAE(T) \equiv (R_{IE} \wedge A(T,\beta,e)) \Longrightarrow Q_{IE}$

- IAI, BSIAI und SIAI entsprechend

zweite Sorte: Hochniveauereignisse können dazukommen

$$
\begin{array}{ccccc}
\mathrm{IE} & \mathrm{SII} & \Longrightarrow & \mathrm{BSII} & \Longrightarrow & \mathrm{II} \\
\Downarrow & \Downarrow & & \Downarrow & & \Downarrow \\
\mathrm{IHAE} & \mathrm{SIHAI} & \Longrightarrow & \mathrm{BSIHAI} & \Longrightarrow & \mathrm{IHAI} \\
\Downarrow & \Downarrow & & \Downarrow & & \Downarrow \\
\mathrm{IAE} & \mathrm{SIAI} & \Longrightarrow & \mathrm{BSIAI} & \Longrightarrow & \mathrm{IAI}
\end{array}
$$

- ersetze E und I durch andere Teilmengen von Hochniveauereignissen und erhalte weitere ESPs mit entsprechenden Implikationsgraphen

von ESPs induzierte Abschlussoperationen

- eine Abschlussoperation
  C: $\wp(E^*) \longrightarrow \wp(E^*)$
  sichert ein ESP zu, wenn $\forall T \subseteq E^*$: ESP(C(T))

- C_{ESP} sei die Menge aller induzierten (minimalen) Abschlussoperationen

- ESPs, für die C_{ESP} einelementig ist:
  die, für die der Ablauf τ', der zu jedem τ existiert, eindeutig bestimmt ist
  also RE, SRI, DE, SDI, IE, SII, IHAE, SIHAI, IAE und SIAI
  im Gegensatz zu RI, DI, BSDI, II, BSII, IHAI, BSIHAI, IAI und BSIAI

bekannte Sicherheitsprädikate zusammenbauen

- *non-inference* (NF) verlangt:
  ein Niedrigniveaubeobachter kann nicht folgern,
  dass Hochniveauereignisse stattgefunden haben

- $NF(T) \equiv \forall \tau \in T \exists \tau' \in LLES(T,\tau): \tau'|_H = \varepsilon$
  $\Longrightarrow NF(T) \equiv RE(T)$

- *generalized non-inference* (GNF) verlangt:
  ein Niedrigniveaubeobachter kann nicht folgern,
  dass Hochniveaueingaben stattgefunden haben

- $GNF(T) \equiv \forall \tau \in T \exists \tau' \in LLES(T,\tau): \tau'|_{HI} = \varepsilon$
  $\Longrightarrow GNF(T) \equiv RI(T)$

bekannte Sicherheitsprädikate zusammenbauen

- *generalized non-interference* (GNI) verlangt:
  zu jeder Verschränkung τ der Niedrigniveauereignisse eines Ablaufs τ_L
  mit den Hochniveaueingaben eines (anderen) Ablaufs τ_H
  enthält LLES(T,τ) eine Vervollständigung mit Hochniveauereignissen,
  die keine Eingaben sind

- $GNI(T) \equiv \forall \tau_L,\tau_H \in T \forall \tau \in interleave(\tau_L|_L,\tau_H|_{HI}) \exists \tau' \in LLES(T,\tau): \tau = \tau'|_{HI}$
  $GNI(T) \equiv RI(T) \wedge IHAI(T)$

- McLeans *separability* verlangt: hohes und niedriges Niveau unabhängig

- $SEP(T) \equiv \forall \tau,\tau_H \in T \forall \tau' \in interleave(\tau|_L,\tau_H|_H): \tau' \in LLES(T,\tau)$
  $SEP(T) \equiv RE(T) \wedge IHAE(T)$

bekannte Sicherheitsprädikate zusammenbauen

- Zakinthinos' und Lees *perfect security property* (PSP) verlangt:
  von niedrigem Sicherheitsniveau aus betrachtet ist es möglich, dass
  gar keine Hochniveauereignisse passiert sind oder
  ausschließlich erlaubte Hochniveauereignisse passiert sind

- $PSP(T) \equiv$
  $\forall \tau \in T \forall \alpha,\beta \in E^* \forall e \in E:$
  $(\tau|_L \in LLES(T,\tau) \wedge$
  $((e \in H \wedge \beta\alpha \in LLES(T,\tau) \wedge \alpha|_H = \varepsilon \wedge \beta e \in T) \Longrightarrow \beta e \alpha \in LLES(T,\tau)))$

  $\Longrightarrow PSP(T) \equiv RE(T) \wedge IAE(T)$

$$\begin{array}{ccccc} PSP & \Longleftarrow & SEP & \Longrightarrow & GNI \\ \Downarrow & & & & \Downarrow \\ NF & & \Longrightarrow & & GNF \end{array}$$

Kompatibilität von SPs mit anderen Systemeigenschaften

- in realen Systemen nur bestimmte Menge T von Abläufen sinnvoll
- T muss für eine vom SP induzierte Abschlussop. abgeschlossen sein
  $P = C_{SP}(T)$
- bestimmte Sicherheitsprädikate sind mit bestimmten
  Arten von Informationsfluss von unten nach oben inkompatibel
- gelte für zwei SPs: $SP_1 \Longrightarrow SP_2$ (SP_2 nicht restriktiver als SP_1)
  wenn T kompatibel ist mit SP_1, dann auch mit SP_2
- seien C_1 und C_2 induzierte Abschlussoperationen für SP_1 und SP_2
  wenn $C_2 \circ C_1 \circ C_2 = C_1 \circ C_2$, dann ist $C_1 \circ C_2$ Abschlussop. für $SP_1 \wedge SP_2$
  wenn C_1 und C_2 die einzigen ind. Abschlussop.s für SP_1 und SP_2 sind,
  dann ist $C_1 \circ C_2$ die einzige induzierte Abschlussop. für $SP_1 \wedge SP_2$

Informationsfluss von unten nach oben

- ob poss. Sicherheitsdef. kompatibel mit Informationsfluss, hängt ab von
  der possibilistischen Sicherheitsdefinition und
  der Art des Informationsflusses nach oben

- Auslösung eines Ereignisses auf hohem Niveau durch eins auf niedrigem
  unmittelbar:
    auf bestimmte Niedrigniveauereignisse müssen sofort
    bestimmte Hochniveauereignisse folgen
  sequentiell:
    zwischen zwei Vorkommen bestimmter Niedrigniveauereignisse muss
    die Reaktion auf das erste auf hohem Niveau erfolgen
  überhaupt:
    zu jeder Zeit muss ein (eventuell leeres) Anfangsstück der
    aufgetretenen Kette bestimmter Niedrigniveauereignisse auf
    hohem Niveau bestätigt worden sein

Informationsfluss von unten nach oben

- Verhinderung eines Ereign. auf hohem Niveau durch eins auf niedrigem
  Eingabe:
    auf bestimmte Niedrigniveauereignisse folgt unmittelbar
    keine entsprechende Eingabe auf hohem Niveau
  Ausgabe:
    auf bestimmte Niedrigniveauereignisse folgt unmittelbar
    keine entsprechende Ausgabe auf hohem Niveau

- GNF ist kompatibel mit allem
  NF und PSP ist nur inkompatibel mit unm. und seq. Auslösung
  GNI ist nur inkompatibel mit unm. Auslösung und Eingabeverhinderung
  SEP ist inkompatibel mit allem

- PSP ≡ RE ∧ IAE, wobei nur RE problematisch ist
  ⟹ PGSP ≡ RI ∧ IAE (halbwegs gutes SP, *pretty good SP*)

das halbwegs gute Sicherheitsprädikat PGSP

- PGSP ≡ RI ∧ IAE ist voll kompatibel mit betrachteten Informationsflüssen
  (aber nur wenig schwächer als PSP)

- Überlegung zur weiteren Verschärfung ohne neue Inkompatibilitäten:
  nicht alle Ereignisse aus H\HI folgerbar machen, sondern
  nur die, die wirklich Niedrigniveauereignisse verarbeiten
  ⟹ ersetze „Entfernung von Eingaben“ RI
  durch „Entfernung kritischer Ereignisse“ R(H\H'); wobei H' unkritisch

- $PGSP_{H'} \equiv R(H\backslash H') \wedge IAE$

  $PGSP_{H\backslash HI} \equiv PGSP$

  $PGSP_{\emptyset} \equiv PSP$

inkrementelle Entwicklung sicherer Systeme

- Verfeinerungsparadoxon:
  Verfeinerung eines sicheren Systems (Teilmengenbildung auf Abläufen)
  nicht unbedingt sicher

- erste Möglichkeit:
  nach Verfeinerung gucken, ob Ablaufmenge abgeschlossen ist,
  gegebenenfalls abschließen

- zweite Möglichkeit:
  Schnitt zweier unter C abgeschlossener Ablaufmengen
  ist unter C abgeschlossen