Tipski sistemi u računarstvu

Svetlana Jakšić

Fakultet tehničkih nauka
Univerzitet u Novom Sadu

Sustavi dokazivanja 2012, Dubrovnik

Outline

Outline

Tipski sistemi u računarstvu

Tipski sistem

Statički metod za dokazivanje odsustva određenih ponašanja programa klasifikacijom označenih relevatnih događaja.

Teorija tipova

U logici, matematici i filozofiji:

- za izbegavanje logičkih paradoksa (Russell 1902)
- u teoriji dokaza (Gandy 1976 i Hindley 1997)

Zasnovano na radovima:

- ramified theory of types (Whitehead i Russell 1910)
- simple theory of types (Ramsey 1925)
- simply typed lambda-calculus (Church 1940)
- constructive type theory (Martin-Löf 1973, 1984)
- pure type systems (Berardi 1988, Terlouw 1989, Barendregt 1992)

Primena u računarstvu

Dve grane izučavanja tipskih sistema:

- apstraktna čiji je fokus na pronalaženju veza između različitih tipiziranih lambda-računa i logika; svojstvo terminacije dobro tipiziranih termova
- praktična čiji je fokus primena na programske jezike

Primena u računarstvu

Tipski sistem

Statički metod za dokazivanje odsustva određenih ponašanja programa klasifikacijom označenih relevatnih događaja.

- Statička aproksimacija ponašanja programa tokom izvršavanja.
- Ponekad provera može biti dinamička tj u toku izvršavanja.
- Mogu dokazati samo odsustvo neželjenog ponašanja programa.

`if` <complex test> `then 5 else` <type error>

U različitim jezicima razlčite "run-time type errors".

Na primer: `a : int; a!x`.

Tipski sistemi i dizajn programskih jezika

- karakterizacija željenog ponašanja programa (well-behaved processes)
- konstrukcija tipskog sistema
- subject reduction teorema - teorema o prezervaciji tipa tokom izvršavanja
- type soundness teorema - dobro tipizirani programi imaju željeno ponašanje tj. nemaju grešku

Za šta su korisni?

- otkivanje grešaka
- apstrakciju
- dokumantaciju
- language safety
- dokazivače teorema

Outline

Kontrola bezbednosti i prava pristupa u distribuiranom sistemu sa XML podacima

Mariangiola Dezani-Ciancaglini, Silvia Ghilezan, Svetlana Jakšić, and Jovanka Pantović.

Types for Role-Based Access Control of Dynamic Web Data.
In *WFLP'10*, volume 6559 of *LNCS*, pages 1–29. Springer, 2011.

Philippa Gardner and Sergio Maffeis.

Modelling dynamic web data.
Theoretical Computer Science, 342(1):104–131, 2005.

Mariangiola Dezani-Ciancaglini, Silvia Ghilezan, and Jovanka Pantovic.

Security types for dynamic web data.
TGC, volume 4661 of *Lecture Notes in Computer Science*, pages 263–280. Springer, 2006.

Mariangiola Dezani-Ciancaglini, Silvia Ghilezan, Jovanka Pantovic, and Daniele Varacca.

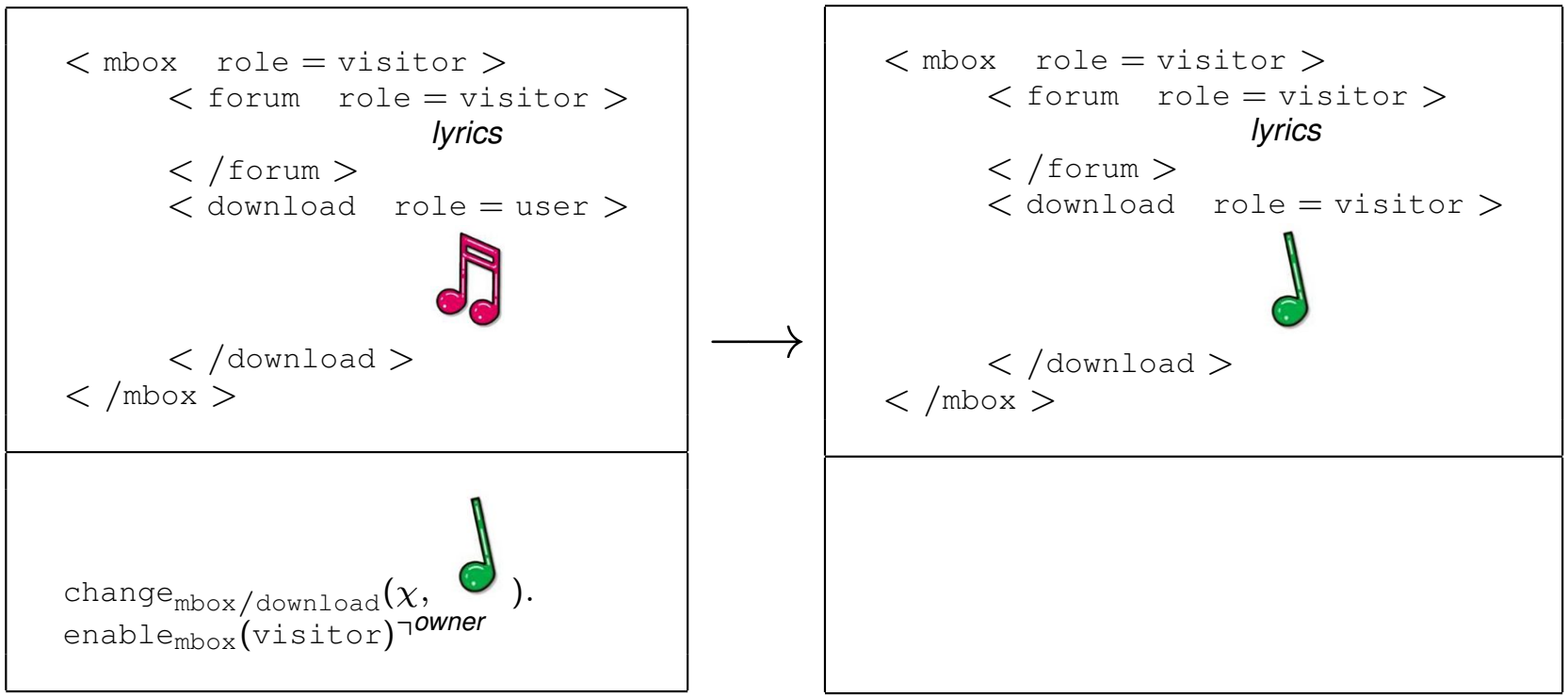
Security types for dynamic web data.
Theor. Comput. Sci., 402(2-3):156–171, 2008.

Silvia Ghilezan, Svetlana Jakšić, Jovanka Pantović, and Mariangiola Dezani-Ciancaglini.

Types and Roles for Web Security.
Transactions on Advanced Research, 8(2):16–21, 2012.

Music Box

Roles: $\texttt{visitor} \sqsubseteq \texttt{user} \sqsubseteq \texttt{owner}$ Policy:$(\{\texttt{visitor}\},\{(\{\texttt{owner}\},\texttt{visitor})\},\{(\{\texttt{owner}\},\texttt{user})\})$



Tipovi

$Loc(\sigma, \mathcal{E}, \mathcal{D})$
$Script(\sigma, \mathcal{E}, \mathcal{D})$
$Path(\alpha)$
$Pointer(\alpha)$
$Tree(\sigma, \mathcal{E}, \mathcal{D}, \tau, \zeta)$

$Proc(\sigma, \mathcal{E}, \mathcal{D}, \rho)$
$ProcRole(\sigma, \mathcal{E}, \mathcal{D})$
$Ch(Tv)$
Net

$$Tv ::= Ch(Tv) | Loc(\sigma, \mathcal{E}, \mathcal{D}) | Script(\sigma, \mathcal{E}, \mathcal{D}) | Path(\alpha) | Tree(\sigma, \mathcal{E}, \mathcal{D}, \tau, \zeta)$$

Pravila tipiziranja

$$\frac{\Gamma \vdash p : \mathit{Path}(\alpha) \quad \Gamma \vdash P : \mathit{Proc}(\sigma, \mathcal{E}, \mathcal{D}, \rho) \quad \alpha \leq \rho \qquad \Gamma \cup \Gamma_\chi \vdash \begin{cases} V : \mathit{Script}(\sigma, \mathcal{E}, \mathcal{D}) \text{ or} \\ V : \mathit{Pointer}(\beta) \text{ or} \\ V : \mathit{Tree}(\sigma, \mathcal{E}, \mathcal{D}, \tau', \zeta') \quad \alpha \leqq \tau' \end{cases} \quad \text{if } \chi = x^{(\sigma,\mathcal{E},\mathcal{D},\tau,\zeta)} \text{ then } \zeta \leq \rho}{\Gamma \vdash \mathtt{change}_p(\chi, V).P : \mathit{Proc}(\sigma, \mathcal{E}, \mathcal{D}, \rho)} \quad \text{(Change)}$$

$$\frac{\vdash l : \mathit{Loc}(\sigma, \mathcal{E}, \mathcal{D}) \quad \vdash T : \mathit{Tree}(\sigma, \mathcal{E}, \mathcal{D}, \tau, \zeta) \quad \vdash R : \mathit{ProcRole}(\sigma, \mathcal{E}, \mathcal{D})}{\vdash l[\![\ T \parallel R\ ]\!] : \mathit{Net}}$$

Prezervacija tipa

Subject reduction teorema

Ako $\vdash \mathbf{N} : \mathit{Net}$ i $\mathbf{N} \to \mathbf{N}'$, onda $\vdash \mathbf{N}' : \mathit{Net}$.

Osobine

Korišćenjem tipskog sistema pokazali smo da važe sledeće osobine:

1. stabla sa podacima i procesi sa ulogama se slažu sa politikom lokacije na kojoj se nalaze;
2. proces može da migrira samo na lokaciju sa čijom politikom se slaže;
3. proces sa ulogama može da čita i modifikuje samo podatke kojima može da pristupi;
4. proces sa ulogama može da doda ili oduzme uloge u stablu sa podacima samo u skladu sa politikom lokacije.

Kontrola privatnosti u sistemu sa RDF podacima

Silvia Ghilezan, Svetlana Jakšić, and Jovanka Pantović.

Privacy for linked data.
Submitted, 2011.

Ross Horne and Vladimiro Sassone.

A typed model for linked data.
Technical Report, February 2011.

Ross Horne and Vladimiro Sassone.

A verified algebra for linked data.
In *Proceedings of FOCLASA*, volume 58 of *EPTCS*, pages 20–33, 2011.

Owen Sacco and Alexandre Passant.

A privacy preference ontology (ppo) for linked data.
In *Proceedings of the Linked Data on the Web Workshop (LDOW2011)*, 2011.

Linked Data

- Web of Linked Data
- Tehnologije: URIs, RDF, SPARQL,...
- W3C projekat: Semantic Web
  `http://www.w3.org/standards/semanticweb/`
- Do sada odjavljeni podaci na inetrnetu: mediji, publikacije, prirodne nauke, geografski podaci, DBpedia, elektronska uprava, sadržaj generisan od strane korisnika društvenih mreža i blogova,...

Privatnost

- Alan Westin je definisao privatnost kao "mogućnost kontrole ko ima pravo pristupa podacima i kome se ti podaci mogu proslediti".

- Privatnost ne mora da uključuje samo privatan status nekih podataka već i značaj ili nedostatak značaja tih podataka za neku grupu kao i sposobnost pravilnog razumevanja.

Ideja

- Sačuvani podaci $\underline{D}$
- Politika privatnosti D_1
- Profil korisnika C
- Query P

$$\underline{D}^{D_1} \qquad \{P\}_C$$

Tipski sistem, između ostalog, odezbeđuje da se promena politike privatnosti podataka vrši u skladu sa politikom privatnosti celog grafa (baze) kome ti podaci pripadaju.

Kontrola curenja memorije

Svetlana Jakšić and Luca Padovani.

Exception handling for copyless messaging.
Submitted, 2012.

Viviana Bono and Luca Padovani.

Typing Copyless Message Passing.
Logical Methods in Computer Science, 8:1–50, 2012.

Kontrola curenja memorije

- operativni sistem Singularity
- Sing#
- programiranje se vrši komuniciranjem pokazivača na poruke preko kanala

Kontrola curenja memorije

Well-behaved procesi su oni koji kod kojih nema curenja memorije, grešaka u memoriji i grešaka u komunikaciji.

- *Curenje memorije* se pojavljuje kada postoji alocirani deo memorije na koji nema pokazivača. U ovom slučaju alocirani region nema vlasnika, zauzima prostor, a ne može mu se više pristupiti.
- *Greška u memoriji* se pojavljuje kada pokazivač pokazuje na lokaciju u memoriji koja više ne postoji ili nije ni postojala.
- *Greška u komunikaciji* se pojavljuje kada proces primi podatak neočekivanog tipa.

Kontrola curenja memorije

- session types = contracts
- Subject reduction teorema ima složeniju formu.
- Type soundness teorema potvrđuje da dobro tipiziran sistem ne poseduje nijednu od gorenavedenih grešaka.